House of Lords
House of Commons
Joint Committee on the Draft Communications Data Bill

Draft Communications Data Bill

Session 2012-13

Oral evidence
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
List of oral evidence

Home Office Officials [Richard Alcock, Charles Farr and Peter Hill] (QQ 1-96) 4

Mr David Davis MP, Big Brother Watch [Nick Pickles], Open Rights Group [Jim Killock] and Privacy international [Dr Gus Hosein] (QQ 97-126) 36

HMRC [Donald Toon], Metropolitan Police Service [Cressida Dick], ACPO [Gary Beauchridge], SOCA [Trevor Pearce] and CEOP [Peter Davies] (QQ 127-185) 51

FSA [Daniel Thornton], LGA [Councillor Paul Bettison], UKBA [Gillian McGregor] and Gambling Commission [Nick Tofiluk] (QQ 186-220) 72

Nick Pickles, Jim Killock, Rachel Robinson and Angela Patrick (QQ 221-274) 85

Professor Anthony Glees and Dr Julian Richards (QQ 275-329) 111

Professor Ross Anderson, Professor Sadie Creese, Professor Peter Sommer and Firewolf [Glyn Wintle] (QQ 330-416) 129

Everything Everywhere [Jonathan Grayling], Telefonica UK [Bob Hughes], BT [Mark Hughes], Vodafone [Vodafone] and Virgin [Simon McReady] (QQ 417-508) 165

IPSA [Nicholas Lansman], LINX [Malcolm Hutty] and Jimmy Wales (QQ 509-546) 192

Google [Sarah Hunter], Hotmail/Microsoft [Stephen Collins], and Yahoo! [Emma Ascroft] (QQ 547-600) 211

Facebook [Simon Milner], Twitter [Colin Crowell], Skype/Microsoft [Stephen Collins], and Tor Project [Steven Murdoch] (QQ 601-659) 229

Interception of Communications Commission [Sir Paul Kennedy and Joanna Cavan] (QQ 660-690) 245

Information Commissioner [Christopher Graham] (QQ 691-713) 267

Demos [Jamie Bartlett] (QQ 714-734) 281

Lord Carlile of Berriew (QQ 735-749) 293

Henry Porter, Duncan Campbell and Paul Heritage–Redpath (QQ 750-783) 300

Crown Prosecution Service (QQ 784-839) 316

Home Office Officials [Richard Alcock, Charles Farr and Peter Hill] (QQ 840-918) 328

Home Office Officials [Richard Alcock, Charles Farr and Peter Hill] (QQ 919-933) 345
BAE Systems Detica [Martin Sutherland and John Davies] (QQ 934-1012) - Evidence taken in private and not published 356

Trefor Davies, David Walker, Caspar Bowden and Privacy International [Dr Gus Hosein] (QQ 1013-1067) 357

National Policing Improvement Agency [Steve Higgins], Greater Manchester Police [Sir Peter Fahy and Alan Lyon], CEOP [Peter Davies], and PSNI [David Stevenson] (QQ 1068-1140) 375

Secretary of State for the Home Department [Rt Hon Theresa May MP] (QQ 1141-1207) 398
Oral evidence

TUESDAY 10 JULY 2012

Members present:

Lord Blencathra (Chairman)
Lord Armstrong of Ilminster
Baroness Cohen of Pimlico
Lord Faulks
Lord Jones
Lord Strasburger
Mr Nick Brown
Michael Ellis
Dr Julian Huppert
Stephen Mosley
David Wright

Home Office Officials [Richard Alcock, Charles Farr and Peter Hill] (QQ 1-96)

Examination of Witnesses

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

Q1 The Chairman: Welcome to this afternoon’s session. We begin our first public evidence session with officials from the Home Office. Welcome, Mr Alcock, Mr Farr and Mr Hill. Perhaps, gentlemen, I could ask you to introduce yourselves and say what your role and function is and then I will ask if you wish to make any opening statement before we begin the questions session.

Peter Hill: I am Peter Hill. I am the Head of the Pursue Policy and Strategy Unit in the Office for Security and Counter-Terrorism. Among my responsibilities is oversight of the policy and law in relation to covert powers, including communications data.

Charles Farr: Hello. My name is Charles Farr. I am Director General of the Office for Security and Counter-Terrorism.

Richard Alcock: I am Richard Alcock. I am the Director of the Communications Capabilities Development Programme.

Q2 Michael Ellis: Mr Farr, the previous Government enacted pieces of legislation that affected the area of communications. I am referring now to the Regulation of Investigatory Powers Act—RIPA, as it is sometimes referred to. What are the key facts that lead the
Home Office to believe now that powers in this draft Bill, the Communications Data Bill, are necessary?

*Charles Farr:* One aspect of RIPA, as you know, concerned the access which public bodies may obtain to what we call “communications data”, which we understand, and you know this very well, to include information about a communication—of course, not the content of the communication itself. In that particular area, RIPA, to some degree, has been overtaken by technical change in the communications industry and changes in the way people use communication, with the result that the data that public authorities have had access to in the past is no longer as readily available to them as it used to be, for a variety of reasons that I am happy to go into now if you would like me to do so.

**Q3 Michael Ellis:** Perhaps you could elaborate.

*Charles Farr:* The change in communications usage is, very simply, one that involves a shift from mobile phones of an old kind, if I can put it like that, to computer-based communications. As that transition has happened, so have two or three other consequences of it. First, communications service providers—CSPs, if you will—no longer retain, for their own business purposes, communications data as we know it. Indeed, sometimes not only do they not retain it, but they do not generate it either. Therefore, when public authorities seek access to that data, on a case-by-case basis, there is nothing to which they can get access, because it is not retained by the provider.

**Q4 Michael Ellis:** So, previously, say 30 years ago, BT may have kept data because they needed it in order to bill people correctly.

*Charles Farr:* Yes.

*Michael Ellis:* But today, data is not kept in the same way, so if you were to seek relevant information, the service providers would not necessarily be able to provide it.

*Charles Farr:* That is correct. So, in the old days of a single telephone line in your home or office provided by, pretty much, a single provider, that single provider required quite a lot of communications data to enable the provider to bill you appropriately on a call-by-call, duration-by-duration, destination-by-destination basis. As we move from the world of old-style telephony to the world of computer-based communication, that business model ceases to apply. I suspect many people in this room will have experienced this; you no longer pay per transaction, if I can put it that way, or per communications event. You pay per month or per year.

**Q5 Michael Ellis:** You pay per month to have a broadband service rather than per call.

*Charles Farr:* Yes, and the provider has much less interest in aspects or some bits of data than used to be the case. I think the provider will, very often, obviously be interested in your subscriber identity, if I can put it like that—who you are and where you are—for billing purposes, but may not be interested in very much else, in fact.

**Q6 Michael Ellis:** So, Mr Farr, is it a correct characterisation that the Home Office is seeking not to extend powers deeper into the area of privacy but simply to prevent a further degradation of powers that were previously available and that you say are declining?
Charles Farr: It is certainly true that a capability gap, if I can put it like that, has opened and public authorities can no longer get access to the data that they would want. As you know, we have put, based on our survey of the relevant organisations, a figure of 25% of data that organisations would like to get access to but cannot.

Q7 Michael Ellis: Can I press you on that 25%? How much of that 25% that you can now no longer obtain is due to non-compliance by the communications service provider and how much is simply not available because those CSPs do not have the data?

Charles Farr: I do not have the exact proportions, but in large measure it is because the data is no longer available. Sometimes it is also because the legislation under which we are operating, RIPA, but in particular—I am afraid this is where it gets more involved—the Data Retention Directive, is not clear about what data the provider should retain even where the provider has generated it and could, in theory, retain it if the provider chose to do so. So there is, if you like, a technical problem, which I have referred to already, lack of data; that is then compounded by a legal problem that the EU DRD, the governing legislation on retention, is not very clear about what IP data, computer-based data, the provider should retain as well. So you are hit by two issues and both of those affect the capability of public bodies to get access to the data they need.

Q8 Michael Ellis: If the DRD is not clear, does that not also operate as a negative in the other direction, in that service providers could retain information for longer than would be required, for example, or longer than they should do?

Charles Farr: I think the ambiguity in DRD is certainly making for a variety of different practices across countries in Europe which have transposed DRD, which is almost all, and there are different interpretations by those countries of what companies should retain, particularly regarding IP data. I emphasise that on mobile telephony of an old kind and fixed-line telephony the DRD is much more specific. So, to that extent, the answer to your question is yes.

Q9 Michael Ellis: Is there evidence that the changes proposed by this Bill would make available the data requested in that 25%?

Charles Farr: Yes. As part of the business case that we do—Richard is responsible for that and it comes through me—it goes first to the Home Office Business Board, then to the Treasury and to other departments. We have to make, obviously, a really detailed business case explaining how much this is going to cost, what benefits we might accrue from it and, of course, the technical feasibility. We are clear that the measures proposed in this legislation would, first, stabilise the degradation and then, over a period of time, improve our coverage to a figure of what we think should be in the region of 85%, as opposed to 75%, which is where we are now, probably over a period going out to 2018.

Q10 Michael Ellis: On the subject of the communications data that is currently used, we are told that under RIPA—this is the pre-existing legislation; it is legislation that has been on the statute book for some years—in 2010 there were over half a million requests for communications data: 552,550. Could you elaborate on what a single request can comprise of?
Would one of those half a million requests cover more than one person and would the investigation of one person generate more than one request?

**Charles Farr:** There is a group of questions in that; let me try to unpack it as best I can. First of all, a single request for data can be for more than one item of data. Let me give you an example: requests are about instruments, not people, for the simple reason that, generally speaking, you may not know who owns an instrument before you seek the data from the instrument concerned. When you request data about that instrument, that communications instrument, you might request both the subscriber and, perhaps, where that instrument was at a particular time on a particular day. So a request regarding a specific instrument may elicit and be intended to elicit more than one item of data about the instrument in question. Is that clear?

**Q11 Michael Ellis:** Yes, but could an inquiry relate, therefore, on more than one occasion to the same instrument?

**Charles Farr:** It is certainly possible that over the course of a criminal investigation—and, as you know, 99% of requests for data are from the police or the security agencies in the context of an investigation, criminal or otherwise—more than one request could be made about the same instrument seeking different information about it, because it may appear, as a result of the first data request, that that instrument is important and clearly centrally relevant to the investigation. At that point, the investigator may well feel it is both necessary and proportionate, which are the two criteria that will be in his or her mind, to go back in and get more data, so yes.

**Q12 Michael Ellis:** So half a million requests for information or for communications data does not represent half a million people.

**Charles Farr:** That is certainly true, because many of the people who are under investigation in a criminal investigation will use numerous telephones, or instruments I should say—it is not just telephones—at one time and dispose of them very regularly. So it might be that a single person, over the course of an investigation lasting three months, gets through 30 or 40 different instruments, all of which generate, for the investigator, different requests. So it is certainly true that 500,000 requests do not equal 500,000 people. It is very hard to come up with a figure about how many people they do relate to and we are doing some more work on that in an attempt to better inform you.

**Q13 Michael Ellis:** Perhaps you would let us know that figure, if you can.

There was a snapshot survey in 2010 by the Home Office, which indicated that 17.3% of police communications data requests were for non-serious crime. Could you say something, Mr Farr, or one of your colleagues, about what is meant by “non-serious crime”? Further to the points you were just making, for example, do you know, in the average murder investigation, how many data requests there might be and relate that to what is meant by “non-serious crime”?

**Charles Farr:** If I can take the second question first, in an average murder investigation it is difficult to come up with an average figure, but from the work we have done it is very possible that the number of comms data requests could be between 500 and even 1,000. Generally speaking, in a murder investigation they may just be for subscribers, in the first instance,
trying to find out, very simply, who a victim has been in contact with in the preceding year, a
year being the outer limit for the time for which data is being returned, at least under DRD. So, yes, a single investigation can create a lot of data for a single—

Q14 Michael Ellis: What about the non-serious crime?
Charles Farr: There is no single statutory definition of “serious crime”, unfortunately. That complicates my answer to your question, but non-serious crime could include, for example, in this particular context, harassment, stalking, aggravated theft, assault on a police officer, and some aspects of fraud. All of them could well be non-serious crime.

Q15 Michael Ellis: So perhaps crimes that would be dealt with in the magistrates’ court rather than the Crown Court.
Charles Farr: They could be, yes.

Q16 Michael Ellis: How many of the half million requests were not for criminal investigations at all? Do you know that?
Charles Farr: 99% of applications for communications data are made by the police or the security services. Not all of those, of course, are made in the context of a criminal investigation. A proportion, I think, from recollection—my colleagues may have the information in their head—but somewhere around 6% or 7% are for missing people and people at risk and in danger. I am just checking my figures: 5.65%. 1% of communications data only is used by or represents applications by organisations other than the police and the agencies. Of that 1%, the two biggest chunks are local authorities, one, and the Financial Services Authority, two. The types of data that local authorities get we can then talk to you about or send you the details of, if you wish, but most local authorities’ requests for data are for subscriber data; it is well over half.

Q17 Michael Ellis: Is this for such things as benefit fraud and the like?
Charles Farr: Yes. Local authorities may use simple forms of communications data, if I can put it that way, to investigate those crimes—generally less than serious crimes—for which they and not the police are responsible. That could include, certainly, benefit fraud, trading standards crime, and some antisocial behaviour as well.

Q18 Dr Huppert: Firstly, Mr Farr, can I apologise? I am going to have to leave shortly to present a Bill in the Commons. I just have two, hopefully, quick questions, if I may. The first one is just to understand the scope of a request. How broad could a request be? Could a request be, for example, to get all the information from every subscriber to a service for a period of a week? Would that be possible within the current law?
Charles Farr: No.

Q19 Dr Huppert: That is very helpful. My second question is about the other serious crimes that Mr Ellis was referring to. The Chief Constable of Derbyshire, Mr Creedon, who is the ACPO lead in the area, said last month that he would consider it perfectly appropriate if he saw somebody texting or using a mobile phone while driving to use the communications data
for that. Is that the sort of thing that you and the Home Office would envisage this being for as a non-serious crime?

_Charles Farr:_ I think it is fair to say that we do not think that use would be central to this legislation, and this legislation clearly has not been planned with that in mind. That being said, it is common practice, in the event of a car accident involving fatalities, for communications data to be obtained to try to understand whether the people involved in that crash have been using telephones at the time of the crash itself. So, to that extent, yes, but I would not want to overstate it at all.

_Q20 Dr Huppert:_ Mr Creedon was implying it would be a standard use when you saw somebody driving along using a phone. You would not accept that?

_Charles Farr:_ I hesitate to contradict Mr Creedon. I think you would have to demonstrate necessity and proportionality; let me put it like that.

_Peter Hill:_ The figures certainly do not bear that out.

_Q21 The Chairman:_ Are you, therefore, worried about function creep? That is, you give the police or the security services the power to deal with terrorism, serious crime, paedophiles—the high-level stuff—and within minutes of the Home Secretary’s announcement at the press conference, Mr Creedon was suggesting that speeding motorists ought to be caught as well. Does that concern you, the general point about function creep?

_Charles Farr:_ I think the application process used by the police to get hold of communications data, in my experience and our experience of it, is a thorough and really serious bit of work. The applying officer has to seek authority in written form, justifying the request on the grounds of its necessity for the investigation and its proportionality to the office that is being committed. That application has to consider collateral intrusion, the degree of innocent persons’ data that is going to be acquired. That has to be signed off by a senior officer in the police force, a superintendent or an inspector, and it has to be verified by what we call a single point of contact—inevitably the acronym is SPOC.

_Q22 The Chairman:_ I accept all of that, Mr Farr, but speeding motorists are a far cry from terrorism, serious crime and paedophiles.

_Charles Farr:_ If we look, Mr Chairman, with permission, at the work we have done more recently on the use of communications data, I think it does bear out my point that speeding motorists really do not figure on the list. 27% of data for which applications are made and obtained is for drugs-related offences, 15% is for property offences, arson, armed robbery, theft, 12% is for financial offences, 10% is for sexual offences, 6% is for homicide, 5.65% is for missing persons, 5% is for harassment, 4% is for offences against the persons, and 4% to 5% is for explosives. Speeding is not mentioned.

_Q23 The Chairman:_ So you would be happy to see the Bill toughened up then in terms of proportionality, or some of these cases excluded.

_Charles Farr:_ Your Committee will obviously have a view on that. I think that the police process for determining necessity and proportionality is an effective one, but you will obviously come to your view on that.
Q24 Lord Armstrong of Ilminster: I can understand that the police might want to know whether a motorist has been using his mobile phone if that was thought to have led to a fatal accident in which somebody was killed. I would have more doubts about it if it was just looking after speeding motorists where there was no such event. I wonder if you could comment from that point of view.

The other question is you said just now that there is no definition of “non-serious crime” and I understand that, but in other contexts people have used the length of minimum sentence as a definition of non-serious crime and I wonder if that could be used in this instance as well.

Charles Farr: You are absolutely right, of course. Perhaps I could just ask, with your permission, if Peter could comment on that. We went through a process of looking at definitions of serious crime for the Government in the context of the review of CT powers, you may remember, in January last year. May I just come back to the speeding motorist? I emphasise that an applicant from the police service has to demonstrate necessity and proportionality, otherwise the application will not be approved. Applications are refused; the Interception of Communications Commissioner’s report, due out next week, will give a number, I think for the first time, of applications which are refused. If the necessity argument is not made out, and I personally find it hard to envisage circumstances where speeding per se would require communications data, then the application will not go through. That will then be reviewed, as you know, by the Interception of Communications Commissioner, who will look at the requests and determine whether, indeed, the test of necessity and proportionality have been met. I understand the concern. I do think the arrangements that are in place should address it.

May I just ask Peter to comment on the serious crime question?

Peter Hill: Two quick points. The first is on the data that you referred to, the 2010 survey. First, I think it is worth bearing in mind it is a two-week snapshot, so it is an indication, no more than that. Second, there are shortcomings in that, in that there is no definition or indication of what the people reporting in the survey defined as serious versus non-serious, so that is its limitation. In the study that we are conducting now, and that we hope to let you have data on later this month, we avoid that by simply listing the offences under which data is being requested. That should give a much more detailed picture of what this communications data is being used for.

Secondly, you are absolutely right. There is no single definition of serious crime on the statute book. There are a number of definitions, some based on a list, some based on a tariff. One could introduce, as you say, a minimum threshold. I think the two issues you might want to consider there are: what is the threshold and what falls below it? For example, under most definitions based on a custodial sentence, something like harassment or stalking, which are communications crimes, would not meet that criterion and yet they can have an incredibly damaging impact on the victim, and, of course, they can escalate into far more serious crimes. We know of cases where that sort of harassment—40 or 50 phone calls a day, stalking someone in the street—does turn into a far more serious crime. So you would have to somehow find a way of managing that investigative process whereby you start with a less serious crime and end up with a very serious one. That is not to say it could not be done, but you would obviously lose the ability to use the information for a number of crimes that either
people consider quite important or have the potential to lead to the investigation of more serious crimes.

Q25 Lord Armstrong of Ilminster: It was once said by a Metropolitan policeman that in Devon and Cornwall bicycle theft was serious crime. Can we be reasonably confident that bicycle theft would be excluded for the purposes of this legislation?
Charles Farr: Yes.

Q26 The Chairman: If I may follow up on Lord Armstrong’s point, I think he is making a point of principle that it is not just bicycles, but less serious crime. Would you, in certain circumstances, if we could get the definition right, be willing to dump the less serious crime part out of the Bill?
Charles Farr: I think Peter has talked to the issue. I suppose the question is: less serious crime from whose perspective? If you are being harassed with 50 telephone calls a day and you have a legitimate fear of subsequent assault, I do not know whether you would consider that to be such a less serious crime that it would justify the police, under any changes to this legislation, not having access to the data that could resolve the threat you face. I would feel uncomfortable with that.

Q27 Lord Armstrong of Ilminster: I can think of trying to exclude less serious crime unless it became part of an investigation where that was thought to be incidental to a more serious crime, which I think was something that you foreshadowed in your previous answer. I just wish to see if there is any future in going down the road of an exclusion of less serious crime unless and until there is evidence to think, or reason to think, that it might be part of a more serious crime.
Peter Hill: I am sure you will have police officers here shortly and you will want to ask them about that. The only point I would make is that the feedback we get from them is that it is often the investigation of the less serious crime that leads to knowledge of a more serious crime, and it is often through the investigation of apparently more minor offences that people who one believes are engaged in more serious criminal activity can be approached. But I am sure those are questions that you will put to the CPS and to the police.

Q28 Lord Strasburger: Going back to your 25% shortfall of information you cannot get your hands on, what proportion of that 25% gap is due to customers choosing to conceal either their identity or their activity, either for nefarious reasons or perfectly innocent reasons?
Charles Farr: Richard may want to comment on that, but perhaps I can just say a few things. I think the answer to that is not very much. If you have the data provided for in this legislation, then you can resolve increasingly anonymous communications, which are a feature of the communications environment in which we live. To put it another way, if you have the right kind of data, issues of anonymisation cease to be a significant problem.

Q29 Lord Strasburger: So is there any risk, if this Bill is enacted, that those with a good reason to conceal their identity or their activity, or those who just choose to do it, will make greater efforts to do so and your gap will reopen?
Charles Farr: If people choose to take greater efforts at anonymisation, that is not necessarily a problem for this Bill. If they are engaged in a criminal activity that we are investigating, then of course, in theory, it may become a problem. I am satisfied that with the techniques that are being developed, which will be facilitated by retention of a kind envisaged in this legislation, many workarounds can be defeated. However, one point I would emphasise, and perhaps I can do it now—I could have done it earlier—is that we are not proposing this legislation on the grounds that it will recover 100% coverage of the communications environment. Those days have gone and you will note my earlier comment that we are not seeking or anticipating that they will return. So there will be cases, of course, where people can find, perhaps temporarily, workarounds to some of what is envisaged here, but I emphasise we still envisage that by 2018, with this legislation, we can stem the capability gap and restore coverage to somewhere approaching 85% of what we need.

Q30 Lord Faulks: Just going back, briefly, to the notion of serious crime, I do not think anybody is concerned with what you might call trivial crime, but is there not a danger if you start defining serious crime, which is essentially rather a subjective concept anyway, that you are potentially going to prevent exactly what you want to achieve, that you already have the safeguards provided by necessity and proportionality and that we would be searching for a chimera by trying to better a definition of serious crime?

Charles Farr: I think that is our view and I think that the concern about the trivialisation of the use of communications data is therefore better tackled through an examination of the application process and the extent to which necessity and proportionality are, indeed, ingrained in the system. That feels, to me, a more likely route to avoiding trivialisation than defining or redefining serious crime, which, as you rightly say, is fraught with hazard. I personally believe that the necessity and proportionality tests are met by the users who use most of this data—the police—but you will come to a view on that.

Q31 David Wright: I am interested in the point you were making earlier about criminal networks or individuals using 20 or 30 or 40 devices. I think one of the concerns people have is that, in order to target this, there is a danger that you would go on a fishing expedition, looking at devices in an area. It is very difficult to pin those devices down to an individual. How do you hone down your investigation? This may be on very serious crime, the other end of the spectrum to some of the lesser crime we have been talking about. How do you ensure that you are targeting the activity properly of those individuals and we are not out on a fishing expedition that captures thousands of other people’s data?

Charles Farr: I am going to sound a bit like a long-playing record. The investigator has to demonstrate to the senior officer that those instruments for which he or she is seeking to obtain data—be it a subscriber, usage data or traffic data—are centrally involved or connected to a criminal investigation. Now, clearly, he or she is going to use all the skills and abilities that they have and, indeed, the training in this—and there is quite a lot of training we provide already—to try to home in on those devices that are more than normally employed. That will be an iterative process. Try to find the phone that is making the most calls, that is most active, which is most closely in contact with the person or people who are at the centre of the investigation and, by a process of elimination, work towards greater amounts of data on the instruments that appear to be focal points. So I think at every step you demonstrate necessity,
you demonstrate proportionality and you work your way towards those instruments that seem more than normally important. I cannot give you much more of an answer on that. Peter or Richard may want to add to it.

Q32 The Chairman: Finally, before we leave these 552,000 requests, could I be clear in my own mind? You are suggesting that that does not relate to 552,000 people. That would be an exaggerated figure. It would be likely to be many fewer people.
Charles Farr: No, not likely; it will relate to many, many fewer people, of that there is absolutely no doubt.

Q33 The Chairman: So one request could relate to more than one person. I am putting it the other way around.
Charles Farr: In theory, yes, because a request might be for an instrument that is certainly connected to more than one person.

Q34 The Chairman: Generally, you are saying that there could be 1,000 requests, but that might relate just to one or two people.
Charles Farr: It could certainly relate to an organised crime gang of, say, 10 people.

Q35 The Chairman: I understand. Are you aware of any circumstances then where the reverse applies: where there could be one or two requests that might relate to 100 or 1,000 people?
Peter Hill: I do not know the details of the applications made by individual officers, but of course they will always have to demonstrate necessity and proportionality. I am trying to think of where one request might cover hundreds of people.
The Chairman: Or thousands.
Peter Hill: I struggle to think of the circumstances where that may apply. What I could think of is, for example, the phone of a murder victim. You want to find out all the calls received by that individual in the hours running up to their death. That could be a significant number of people.

Q36 The Chairman: I will not press you today on this, because we must move on, but I would be grateful if you would do a check back to see if there are any circumstances where one request could relate to hundreds of people or subscribers, or thousands of people.
Charles Farr: I am with Peter. We will obviously do what you want. I cannot see the circumstances. Sometimes it is the case that a single instrument—a single telephone or laptop—is shared among a criminal network, even a terrorist network, because that instrument is regarded as being safe and secure and, therefore, is used by a number of parties, but not to the scale that I think you may be concerned with.

Q37 The Chairman: There would never be circumstances which critics of this Bill would call a fishing expedition where you get a couple of access requests for thousands of people.
Charles Farr: No.
The Chairman: Excellent.
**Peter Hill:** One area I think we will look at for you is whether, for example, in a serious terrorist investigation one is trying to locate an individual who was in a number of places at certain times, and you then try to get the information from those cell sites in order to work out which phone was in those places at those times. Obviously, that could require you getting a large number of individual bits of data, to work out which phone was in those places at the same time. The Bill, just on that point, does have a mechanism which is intended to help reduce the amount of data that the law enforcement agencies would acquire in that context. Rather than needing to get the information from each location, they would ask which phone was in each location, and then the filter would do all the work for them and just give them the information they needed. So the Bill does have a mechanism in it to try to reduce, in those circumstances where large volumes of data might be requested, that volume of data to the minimum that is necessary to answer the question. But I think it is certainly something we can come back to you with.

**Q38 The Chairman:** I think we would like some more information on that in due course. The Home Secretary said, in letters to Members of Parliament and to Peers, and it was the main justification for the measure, that this was necessary on the grounds of national security, detecting serious crime, the economic well-being of the nation and tackling paedophiles. Yet in the draft Bill, Clause 9(6), we have about 10 purposes listed, including public safety, public health and, rather than just the economic well-being of the nation, we have collecting any tax, duty or levy, and things that may damage a person’s physical or mental health. So we are being told the Bill is necessary for large and important reasons of national security, terrorism, serious crime, and yet are you are concerned that part of the Bill has a lot of extra material?

**Charles Farr:** Clause 9(6), which you are referring to, simply, with one exception, transposes purposes that are set out in RIPA. The single exception to that is Clause 9(6)(c), which says, if I may read it, “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)”. That was added because it had been removed from another piece of legislation that had hitherto been used by authorities to get access to communications data. So having removed it from another piece of legislation where it had facilitated access to data, it was replaced here.

On this list of purposes, Chairman, as you say, it is long. I think it is fair to say, as the Home Secretary pointed out, the vast majority of requests for data are in relation either to “a) in the interests of national security” or “b) for the purpose of preventing or detecting crime or preventing disorder” or “c) in the interests of public safety”. It is true that a number of others have been added in, and I am sure you will want to look at those and we will try to give you as much data as we can about the extent to which they have been relevant to particular requests.

**Q39 The Chairman:** Would you accept that, to a certain extent, it does fuel the suspicions of those who are opposed to this Bill that we hear it is for essential purposes—preventing terrorism, serious crime and paedophiles—and yet the list of purposes has a much wider range?

**Charles Farr:** I am looking at the list of purposes in front of me. Some of them seem to have a really narrow range: “9(6)(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, (ii) to obtain information about P’s next of kin” and so on and so forth. In other words, I am not sure that the large number of purposes to which you rightly allude, beyond those core to which the Home Secretary referred, are very expansive. I think rather the opposite: some of them are very specific and somewhat esoteric.

**Q40 The Chairman:** In that case, would you be averse to a warrant system for applying in those circumstances? If there are very few requests, then why not go to a magistrate for a warrant?

**Charles Farr:** I think, given that the numbers are likely to be very low, then technically, logistically, clearly that would be feasible. You will come to a judgment about whether the oversight that a magistrate could exercise—going back to our mantra of necessity and proportionality—is really going to be more effective than the oversight that might be exercised by other authorities, but I accept that there is a case, yes.

**Peter Hill:** If you look at some of the purposes, they are purposes for the preservation of life. They are to find missing and vulnerable people. They are often requests for communications data that are made with great urgency in order to locate somebody. Whatever system one has in place, you will clearly need something that allows you to have an urgent procedure to access the data, and 5% or 6% of data requests, as Charles has said, are for that purpose.

**Q41 The Chairman:** Yes, I accept that, but there are others which are clearly not of an urgent nature. When you were drafting this Bill, did you consider in the Home Office, because of the history of trying to get to this stage in the past, drafting the Bill more tightly, so that it only did include serious crime, terrorism and national security issues?

**Charles Farr:** Yes. We certainly looked, I think it is fair to say, fairly exhaustively at a very wide range of options. I think ultimately what persuaded the Ministers to leave it as is was that the vast majority of requests are for “a) in the interests of national security, b) preventing or detecting crime or preventing disorder” or “e) in the interests of public safety”. Those others seem to have been shown to be necessary in very specific cases, but have not collectively created a significant number of requests. Therefore, if they can facilitate, on occasion, specific investigations they should remain in the Bill, but I am sure your observations on this will be understood.

**Q42 The Chairman:** Finally from me in this section, would you be able to give us a breakdown of the data requests per purpose? So would you be able to give us a breakdown of the data requests relating—I understand you may not wish to do so for national security—to preventing and detecting crime, public safety, public health, and all the categories in 9(6) and can you tell us if there are any which have never been requested?

**Charles Farr:** As I alluded to earlier, we have two pieces of data on this which are relevant to your question. One is a bit of research that was done in 2010 to look at police applications for data under the crime types that they were investigating. The second was a repeat of that bit of work, which we will finalise in the next few weeks and give to you, of course, which again has taken a snapshot around the country over a two-week period of the crime types in connection with which applications for communications data were made.
The tricky bit is that the categories that we have used to indicate for what crime types data has been applied do not correlate one-to-one with the purposes set out in 9(6). We can tell you, and I specified it earlier, what percentage of communications data has been requested in connection with missing persons and abandoned 999 calls. I have said already 5.6%. That, I think, is what I would understand to be a part of the public safety component.

If I may, we can write to you with our survey, mapping wherever we can the survey on to the purposes and I think that will answer your question.

Q43 The Chairman: That would be helpful and, if you can widen it beyond the police into the public health and the other aspects, the other purposes listed in 9(6), that would be helpful.

Charles Farr: We will do as much as we can.

Q44 Baroness Cohen of Pimlico: Along the stretch of the Bill, what comes under the term “communications data” as drafted? Would it capture a web activity log, for example? There is a suggestion in the media you capture the content of a postcard, which perhaps you cannot have intended. What is your view about what is the stretch of communications data?

Charles Farr: I can deal with the second question very easily. It does not capture the content of anything, a postcard or an e-mail. So that claim is incorrect.

Baroness Cohen of Pimlico: It did sound strange.

Charles Farr: It is strange and it is not in the legislation. On web logs, or web activity logs, as they are called, yes, communications data does capture information demonstrating or indicating the websites to which a device has connected. It does not then enable a public authority to see what has happened within that website unless a communication is involved. Let me try to put it in another way, if I may. Communications data will show which website you have accessed and will show a communication, if you have made a communication using a website. It will not otherwise show the pages of the website or other aspects or parts of the website that you may have visited simply as a reader.

Q45 Baroness Cohen of Pimlico: To use my simple-minded example, I am a regular user of the Ocado website, so the data will reveal that.

Charles Farr: Yes.

Baroness Cohen of Pimlico: But not the contents of my grocery order.

Charles Farr: No.

Q46 Baroness Cohen of Pimlico: Is there anything else I have not thought of that communications data, in fact, spreads to cover? Web activity logs I think one might have thought of.

Charles Farr: I should say, by the way, that this legislation does not change the definition of “data” in respect of web activity logs. It already was accepted in the definition of “communications data” that communications data includes web activity or web logs. There is no other respect in which the definition of “communications data” has changed in this legislation.
Q47 Stephen Mosley: When it comes to cryptic communication, for instance, SSL or something, the encrypted communications data might be in the content of that communication. How is that classified?

Richard Alcock: Through the Bill, we will only be able to store communications data. The means by which we access communications data, our preferred route, will be working in partnership with the communications service providers, who will hold unencrypted data on their own services, i.e. the services that they are providing for their customers. We will be working with them to retain, in some cases, some aspects of communications data and, in that case, it is very easy to separate content from CD. Though I must stress, through the Bill it is illegal for us to collect content. We will only be able to retrieve and store communications data. We will not be applying any systems that cannot reliably extract CD from content through whatever data streams. So, in essence, by working with communications service providers, we can ensure a very reliable means by which we can ensure that we only collect communications data and store that appropriately.

Q48 Lord Faulks: I want to ask you about overseas CSPs, or rather CSPs that are based overseas. Technically, the Bill extends to them. How realistic is it to pursue them for potential breaches of duty?

Charles Farr: If I may, before we get to the question of how realistic, I suppose the prior question is whether that is going to be an issue at all. We have already, of course, relations with many, but by no means all, overseas providers, including those who are household names and are the big suppliers into this country. We have that relationship, for all sorts of reasons, under existing legislation. Those relationships are co-operative and collaborative and, as some of those providers have made clear, they provide data, to the extent that they can—I would emphasise that—in accordance with existing legislation. It is our hope and expectation that that collaborative relationship would continue and it would be part of the purpose of this legislation to facilitate that wherever we can.

You are right, however, that 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 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.

Q49 Lord Faulks: At the moment, what percentage of requests for communications data from overseas-based companies are complied with currently?

Charles Farr: I do not have a statistic. We can—

Lord Faulks: Can you give us an idea, please, of the degree of collaboration and co-operation?

Charles Farr: Peter, do you want to touch on some of the issues there?

Peter Hill: Just in terms of framing the answer, the request may not be the best measure, because under the regime we operate, generally speaking, you should not be making a request if you do not believe that the data is going to be there. So, generally speaking, we will expect most requests to be met. The issue that we have is that requests are not made, because people—the single points of contact in the public authorities—do not think the data is going to be there, so there is a self-censorship in requesting internet-related data. They do not think
the data is there, either because it is not retained or because it is not retained in the form that they need it and, therefore, they do not request it. So, generally speaking, one would expect most of the requests made to be met. There will be some that are not and where there is company policy which means they are not being met, that is what we need to work through with the companies to try to up that level. But the bigger issue is that the data that we need is not available—although there are some exceptions—rather than it is not being shared with us.

**Charles Farr:** Typically, with overseas providers, it is a patchwork quilt; they all look a bit different. Some overseas providers do not have the data. Some have the data but do not want to disclose it, because they do not think there is a legal basis to do so. Some will disclose it, but only in the most serious instances, e.g. terrorism or other threat to life. Some may disclose it, but not in a timeframe that we are used to and that is needed in the context of a rapidly moving criminal investigation. Some may disclose it, but in a form that is hard for us to make use of. So there are a range of issues presented by overseas providers. I reinforce Peter’s point that calibrating the service, if I can put it like that, that we get on the basis of requests met or not met is probably going to give an inaccurate picture.

**Q50 Lord Faulks:** I suppose breach of duty is rather a blunt instrument, is it not?

**Charles Farr:** Yes.

**Q51 Lord Armstrong of Ilminster:** Have you assessed the risk that this legislation might either drive service providers overseas in order to escape the obligations under the Bill or that users of communications equipment might seek to use overseas service providers rather than domestic ones in order to escape observation?

**Charles Farr:** On the first issue, if I may, we have a dialogue with the major CSPs in this country. We have it for all sorts of reasons to do with communications data and, indeed, interception, which also falls within our responsibilities. That is a really constructive dialogue, because major providers recognise obligations they have to provide data and, indeed, to facilitate interception. This legislation—the principles of it, the reasons for it, and the background to it—have been discussed repeatedly in that group and, insistently and consistently, we have had the same response: that those providers understand there is an issue here that needs to be addressed. They want to help address it, but they expect there to be legislation to provide a legal basis to enable them to do so. At no point, in my experience, has a major CSP suggested or even implied that they would rather move overseas than work with this legislation.

On your second point, whether people will move, people already do. Criminals and people engaged in criminal activity spend their lives trying to evade systems that we have constructed and put in place, and work that we do with providers, to evade our attention and control, if I can put it in that way. So I do not think the Bill is going to change that; it already happens. I think what this Bill will do is to give us greater ability to manage that problem when we see it.

**Q52 Stephen Mosley:** One of those abilities, of course, will be the ability to put in black boxes on the network in the UK to look at what is happening on some of these foreign services. Could you explain that a bit, because I think it is one area that people have concerns about? If it is encrypted traffic, of course, even if it is looking at the communications data, it is going to have the ability to unencrypt the content as well. Who would own and operate those black
boxes? Would it be private sector communications providers or would it be yourselves or other agencies?

Charles Farr: Perhaps I can go as far as I can and then I will hand over to Richard on the more technical aspects of this.

I just want to be really clear. So-called black boxes—DPI, or deep packet inspection—is not the cornerstone of this programme. It is not a key or the key feature. It is not the central plank of it. The central plank of this programme is a collaborative relationship with service providers in this country and overseas. DPI, black boxes, or whatever other metaphor or language we choose, only come into play in certain circumstances when an overseas provider or the state from which an overseas provider comes, or both together, tell us that they are not prepared to provide data regarding a service which is being offered in this country and which we knew and know is being used by criminal elements of whatever kind. In those circumstances, we have two options. We could, in theory, accept that there will be a communications service here that is being used by criminals to which we cannot get any access or data. That is not the view of this Government. The legislation therefore creates the option, in those circumstances, of putting a black box, using your language, on a UK network across which the data from the overseas provider must move, with the purpose of sucking off that data, under our guidance—“control” is too strong a word—and storing it through that network provider.

To go to your specific questions, we will talk to the network provider in those circumstances, of course. We will work with that network provider on the technology. We will approve the technology that is going to be used. We will approve the programming of that technology to ensure that it does indeed just take data and not content. As Richard has said, the legislation makes it absolutely clear that it would be illegal to take content under the terms of the Bill. The network provider would store the data.

I want to, if I may, get it in perspective. Black boxes, which attract a lot of attention, of course—partly the language—do not and are not the key issue in this Bill.

Richard Alcock: Answering your point about encryption, there are useful elements within an encrypted data flow. There are unencrypted elements, as I am sure you are aware. By the way, the industry use deep packet inspection equipment now, as a matter of course, to look at their networks. They may have deep packet inspection equipment installed right now in the UK to look at performance, look at allocation of services and the like. It may be possible to use existing deep packet inspection equipment, in the encrypted cases, just to look at that aspect of the data stream that is unencrypted, to establish, if possible, the who, when and where—the communications data elements. As I said before, if we cannot reliably extract CD by that route, then we will not do it.

Q53 Lord Strasburger: Is DPI applied to the entire pipe or to the data attributable to a single user?

Richard Alcock: It would be applied, in extreme cases, to particular services that may be transiting that particular network pipe. So it might be a particular service or application that is flowing in that particular network. It would not be down to an individual. It would not be intercepting an individual’s content.

Charles Farr: If I may add, of course the arrangements for public authorities to subsequently get access to that data are unchanged from the norm. In other words, at no point is it possible
to go on a fishing expedition into data that has been acquired off a DPI from an overseas provider. You continue only to have case-by-case access under the usual and existing authorisation route.

**Q54 Lord Strasburger:** So you would require the service provider to filter out the data that did not apply to the individual that you were seeking to monitor.

**Charles Farr:** It would not really apply, I think. The network provider would take off the network the data particular to the service of concern to us and store all that data. We would then apply to the network provider for specific bits of the data that has been so stored, in accordance with usual practice. That bit of the application process would be fundamentally unchanged from the norm.

**Q55 Lord Armstrong of Ilminster:** If I may just revert to the question of the communications data from overseas CSPs, you gave us a reassuring answer, if I may say so, about their willingness to co-operate. Is there any kind of measure of those who will co-operate and those with whom co-operation is difficult or non-existent, a percentage measure or something of that kind?

**Charles Farr:** We are looking at that. I hope that we may be able to give you more information on that as your scrutiny Committee continues its work.

**Q56 David Wright:** I wanted to touch on the public authorities covered by the draft Bill. My understanding is that RIPA and associated orders outline the authorities that have previously been covered. This new Bill would supersede RIPA in some ways. Why have you not put out a comprehensive list of public authorities that you would want to include under the auspices of this Bill? It seems to indicate, in sections of the Bill, there would be powers for additional authorities to be added in. Could you talk to us around how you have come to the view about what public authorities should have access to communications data?

**Charles Farr:** I think the Government took the view that there were four users of communications data—they are the biggest users—who should be on the face of the Bill. That is to say: the police, intelligence agencies, SOCA—NCA in due course—and HMRC. You will recall from our earlier evidence that those collectively consume 99% of data requests in this country. The operative issue is, therefore, what you do with those authorities who seek 1% of data. It is quite a small percentage but, of course, quite a large number, still, of requests: 5,000. The Government has taken the view that those public authorities need to demonstrate, in a sort of zero-based review way, that they have need for the data in this legislation, for communications data, and should make the case for it. We have written to all those public authorities asking them to set out their business case, building on the information that they have previously provided to us—and, by the way, which we published in 2010 in a RIPA consultation document; we are happy to provide that if you have missed it. We are interested in how often they access CD and why, what alternatives may be open to them, and whether they can provide evidence that they use it in a necessary and proportionate way.

We will then assemble the evidence that we collect from that survey, and we assume you will look at it as well, and the Government will come to a decision.
Q57 David Wright: Will we look at it? You assume we will look at it and that was my follow-up: how is Parliament going to have any oversight on that information? I welcome the fact that you are almost using this process as a review back to see what authorities ought to be entitled to access information. I think that is welcome, but how are we going to have some oversight into that? How can you demonstrate to us what criteria you have used, how it has been assessed, and will that come back before Parliament for affirmative action?

Charles Farr: As we proceed with our review and we get responses from those public authorities, you obviously may wish to talk to us further about what evidence we have received.

Q58 David Wright: What is your timescale?

Charles Farr: Peter will know that.

Peter Hill: I think we are hoping to collate the information that we have asked for by the middle of the summer, so when we are back in the autumn we should know what the business cases are that these public authorities are making.

David Wright: I presume you will be presenting that to this Committee.

Charles Farr: I am sure we will be very happy to. I think we had thought, but of course it is not our business, that you might want to speak to some of the heaviest users within that 1% and to look at the business case they may present to you.

Q59 Lord Armstrong of Ilminster: If everybody goes fairly fast, might you consider including some of the other authorities in the Bill rather than waiting for subordinate legislation?

Charles Farr: That will be a matter for our Ministers. I cannot anticipate what they would want to do with that.

Lord Armstrong of Ilminster: Speaking personally, I would rather see it in the Bill, if possible.

Q60 David Wright: I think that is a genuine concern, Lord Chairman. People fear that there is mission creep a little on the matters. The more we can get on to the face of the Bill the better it is, because it clarifies the situation. Maybe that is a debate we need to have as we reach our conclusions and report.

Peter Hill: I am sure you know this, but, as you say, there is an order-making power. Any authorities who are not currently on the face of the Bill who would wish to have access extended to them would be contained in an order, which would be subject to affirmative procedure, so there would be a parliamentary vote. Whether they should be on the face of the Bill is obviously a decision for Ministers. As you say, there is a demonstrative effect. There is also the issue of putting people on the face of the Bill means it is much harder to take them off in future or, if new organisations are formed, there are structural changes, or there are new purposes, it is much harder to make those changes. But, as I say, it is a balance.

Q61 The Chairman: Some of us, who have been around a long time, heard almost those exact words while serving on the RIPA Committee in 2000, where we were dealing with the big four on the face of the Bill and then the Minister, I think, let slip that there were some
other public authorities who could be added as well. Under questioning, he then produced a letter to the whole Committee showing that when the Bill was completed there were about 32 public authorities added. Twelve months later, we ended with 500 added and now we have 650. So I wonder: was I lied to then, or are we being conned now?

**Peter Hill:** I think you have a very clear list of those who might seek access, which is in the existing consolidated order approved by Parliament in 2010. So I think if, collectively, you and we wish to interrogate from a zero base who should have that access, we have the list of the people who we think will want to have that access, and that is the baseline from which to go.

**Charles Farr:** If I may add, of the 1% of requests that we are talking about—5,000 requests plus or minus—I do come back to the point that the main users are the FSA and local authorities. The rest is a fractional number of requests, somewhere around 500. So I think the FSA and local authorities are the key to this. I honestly do not believe that we are surreptitiously trying to insert major users at the last minute.

**The Chairman:** No, but Parliament must be concerned with the half of the 1% and the civil liberties of those people.

**Charles Farr:** I understand.

**Q62 The Chairman:** Would you accept, to a certain extent, that including some of these more intriguing, lower-level cases, some of the more trivial cases, diminishes to a certain extent the importance of having powers for terrorism, serious crime, paedophilia—the big stuff?

**Charles Farr:** I do not know whether the offences under investigation by the Financial Services Authority now, of all times, would be regarded as trivial by comparison.

**The Chairman:** No, but some of the other public authorities of the 650: the Egg Inspectorate?

**Charles Farr:** I think in the case of some of those—I am not aware of the Egg Inspectorate—their usage is barely in double figures.

**The Chairman:** So why should they have the power at all?

**Charles Farr:** Because the double-figure requests that they do make can be very important. If you are investigating an air accident, for example, it is very low usage, but very high dividend.

**Q63 Baroness Cohen of Pimlico:** There is a perfectly good statutory instrument here, which, if we are going to have a new Bill, I would stick in the back of the Bill—a scheduled plonk. Are we planning to do that?

**Peter Hill:** Which statutory instrument are you referring to?

**Baroness Cohen of Pimlico:** Investigatory powers. It has a list of organisations, a very fine list.

**Peter Hill:** That is the starting point from where people might apply and a version of that, if one went with the order-making route, would then be attached to this Bill. I think, as has been said by the Committee, Ministers wanted to take a zero-based approach and not assume that it was going to be agreed that all those who currently have access through the 2010 order would go on and have that access.

**Q64 Lord Jones:** Who has real oversight over the current use of communications data and the use that will be made under this draft Bill? We are asking you: who is able to assure the public and provide evidence to Parliament that the safeguards are proving effective?
Charles Farr: I sense two questions in there. One is an oversight question and one is a safeguards question. If I can perhaps just address the oversight question and you will tell us how much you would like us to talk about the safeguards question.

Lord Jones: You are adept; make your choice.

Charles Farr: Okay, perhaps we can deal with them in that sequence. On the first, oversight of the process, as you know, it is the duty of the Interception Commissioner to keep under review the performance of the duties placed on Communications Service Providers under this Bill—for example, the duty to generate or collect communications data. The Commissioner also provides independent oversight, with his team, of the acquisition of communications data by public authorities and the role of the commissioner will be extended to oversee the new powers, in particular, the collection of further data by industry—CSPs. That will include oversight of testing, regular auditing and inspections.

The Information Commissioner also has a role, particularly on the retention of the data by industry. An Investigatory Powers Tribunal made up of senior judicial figures, which exists already to handle complaints against the intelligence and security authorities, will be extended to cover the provisions here, ensuring that people have an avenue of complaint, should they need it, and independent investigation if they believe the powers have been used unlawfully against them.

The commissioners report to Parliament each year on the use of these powers and their own authorities will be updated to reflect the nature of the capabilities set out in this legislation. That, for me and for us, is the first key way in which oversight of this process is provided to Parliament.

Shall we talk about safeguards? Can I hand over to Peter on that?

Peter Hill: We can obviously give you more information in writing. I am not sure how much you want me to go into, but I would just set out that if you break down the process of the acquisition, the retention, authorisation, and oversight, there are safeguards at each point of the process.

In relation to retention, you will have the order agreed by Parliament following statutory consultation with those affected. You will have the notices detailing what data is to be retained, following discussion with CSPs, and approved by Ministers. You will have all that data destroyed after 12 months. At the storage level, you have that, subject to explicit requirements in the Bill placing obligations on the companies as to the standards for storage. That is overseen by the Information Commissioner. We have talked quite a lot about access, where there is and there will be an approved list of authorities, the purposes for which and the data that they can acquire will be agreed by Parliament and set out in our legislation.

You then have the authorisation process, which is, within those approved bodies, how you get the data, and I think Charles has talked about that. It is the number of people involved in the authorisation process, the considerations that have to be taken into account, the role of the senior responsible owner for the process, and the inspection and auditing of that by the Interception of Communications Commissioner. Of course, a lot of this data will end up in court as part of a criminal prosecution, where it will be subject to the normal rules of disclosure and challenge by defence. There is a filter provided for in the legislation, to try to minimise the data that is disclosed to public authorities to that which is necessary.

There is then, of course, the oversight regimes we have talked about. There is an appeals process, the Investigatory Powers Tribunal. If all that fails, there is a range of penalties set out
in existing legislation, whether that is data protection, computer misuse, or misconduct in a public office. That is a slightly long answer, but I think it is important if you are looking at safeguards, which I am sure you will be, to try to break down the process to what are the safeguards at each stage of that process.

Q65 Lord Jones: It was not over-long, Mr Hill. We need to know just how much you and your colleagues care about oversight and about safeguarding and if you were to write further, you would have the perfect opportunity to put it down. But it is our duty, as parliamentarians, to look at oversight and safeguards. After all, at the end of the day, as Mr Farr said in his previous meeting with us, it is quite simple: it is about liberty; above all else, it is about liberty. Our duty is to ask you these questions and gain from you the kind of informative answer that you have just given to me. If I may go on, on behalf of the Committee, Parliament is going to be asked to pass the Bill without knowing exactly what data is likely to be sought, the technology that will be used to collect it or how it is used in practice. That is how it comes across to us at this stage; we have not had many sessions of evidence-taking. Public authorities will be added by order and the permitted purposes can be varied by order. What is exercising our minds at this moment on these matters, which you have responded to, is whether Parliament will really have any oversight powers.

Charles Farr: If I may, you raise a question about the degree to which you are given information about what exactly this legislation is going to lead to. I would emphasise, as we did in answer to a previous question, that the definition of “communications data” is clearly set out in existing legislation and there is no change to that here. So I would reassure you that there is nothing in this legislation that is going to amend existing definitions of what communications data is. We continue to think of it, as we have done before, in three categories: subscriber data, service usage data, and traffic data. We are happy to send you further details about what exactly those mean, but that will provide the essential context for any order made under this legislation, and there is no intention to change data definitions at all.

Q66 Lord Strasburger: You might have picked up that certain Members of the Committee are concerned about a certain looseness in the drafting of the this draft Bill, and I pick up another one. Clause 4(2) seems to make it possible for data to be retained not just for 12 months but indefinitely; all a public authority has to do is to notify the telecommunications operator concerned that the data is or may be required for the purpose of legal proceedings. So there seems to be quite a big loophole there for a public authority to extend the retention of data indefinitely, just on the basis that it asserts that it might be required for legal proceedings.

Charles Farr: As you know, communications data is evidentiary. It is used as evidence in court and it is essential that the Bill facilitates that process in the future, as it has in the past. That means that data has to be retained until the court procedure takes place, so I see no alternative to having a clause of that kind. If the clause needs to be more tightly drawn, or if there needs to be greater clarity about the evidence or the material that needs to be put forward to support that application, to demonstrate that criminal proceedings are, indeed, in
the offing or planned and that the data is, indeed, intended as evidence, we can take that away and look at that.

Lord Strasburger: I think what I am saying is that my colleagues on the Committee have drawn to your attention various items, like this one, where there is a lot of opportunity for mission creep. I just draw this one to your attention as yet another example of it.

Q67 Dr Huppert: My apologies again for having to present my Bill—successfully on this occasion.

Mr Farr, if I can start off just by talking about the retention period for data, the EU data retention directive gives flexibility, as I understand it, to keep data for between six months and 24 months. Why have you gone for 12 months in this? What was the evidence for that?

Charles Farr: Obviously, we consulted the major users quite widely on this issue and we have also looked at, and have more recent evidence about, the types of data, the purposes for which it is obtained—we have talked to the Committee about that—and, in particular, the period of time for which the data has been retained by the time we seek access to it. We have also correlated those variables together. So we are able to determine, for example, that, as a matter of interest, claims for communications data in connection with terrorism tend to refer to data which has been stored between six months and 12 months, whereas applications for data in connection with certain other crime types, generally speaking, are for data which has been retained for rather less.

So we consulted and we have looked at the data. We can provide you with the data that is relevant to the latest survey that we have done. In summary, we are satisfied that data retention for a year is required across the range of crime types in connection with which data is applied for, and there is a significant amount of data at the outer end of that period, i.e. between six months and a year, for which the police need access.

Q68 Dr Huppert: I hope you will be able to share all of that data with the Committee and the wider public. Can you give me a sense: of the 552,550 data requests in 2010, how much was, say, less than a month old? Was any of it more than a year old?

Peter Hill: Was that in relation to 2010?

Charles Farr: Yes.

Peter Hill: In relation to 2010—

Dr Huppert: I will take 2009 if you have it.

Peter Hill: Let us take the data that we think we will have towards the end of this month. The data for 2010, around 30% of that was accessed between six and 12 months.

Dr Huppert: Are you saying you do not have the full year’s data?

Peter Hill: The data on the age of data is based on the snapshot surveys. It is not reported in the Interception of Communications Commissioner’s report.

Q69 Dr Huppert: Perhaps I am misreading the Data Retention (EC Directive) Regulations 2009, 9(2)(b), which says that the public communications provider must provide the time between data being retained and requested for every single incident. You must collect that data.
Peter Hill: We return that data to the Commission and the last return we made was for 2010. So the last return that we made to the Commission relates to—so the last data that we have, in addition to the data I was about to give you, related to 2010.

Q70 Dr Huppert: So for 2010 you have full figures for all of those 550,000.
Peter Hill: Yes.
Dr Huppert: And you could share with the Committee the age profile for all of that.
Peter Hill: So we can share with you the age profile for what we know about the 2010 data and, in relation to the 2010 data, around 30% of that was for data between six and 12 months—sorry, for more than six months.
Dr Huppert: So some of it was more than 12 months.
Peter Hill: Yes. So, we cannot require the retention of data after 12 months, but, for example, in relation to subscriber data, businesses may need that for their own business purposes. So 70% was for up to six months and six and beyond was 30%.

Q71 Dr Huppert: If you have all the data, I think it would be very useful to have the breakdowns in number of units. It seems to me that a lot of it would be, in many cases, data within the last week for a missing person investigation.
Charles Farr: Just to be absolutely clear, in the case of terrorist inquiries, there was a significant amount of data required, which has been stored for significantly longer than a week and, generally speaking, between six months and a year. A criminal investigation, particularly an investigation in terrorism, would be very seriously hampered by the reduction of data retention periods to a period of a week or more.

Q72 Dr Huppert: Mr Hill says he has the data to back that up, so I hope you will be able to send it to us and we will be able to look at it for ourselves.
Peter Hill: Yes. The more serious crimes and the more complex crimes generally access data in that later period more than with more simple crimes.

Q73 Dr Huppert: I look forward to seeing the data. Can I then move us on to the other issue—I do not want to take too much time, having missed so much—about costs? The Home Office estimate is that the cost of this Bill as it currently is would be £1.8 billion over the next 10 years. It seems to be very unclear what is included within that cost, partly because it is not yet clear whether you would be able to obtain data by negotiation or whether it would require significant infrastructure, DPI techniques and so forth. What does that £1.8 billion cover?
Charles Farr: We have talked about DPI and when DPI might be used and the circumstances in which it would be used, and I emphasised, of course, that DPI is not central to this legislation. So the likely areas of expenditure are as follows: (a) new systems to enable CSPs to store and process data, including not only telephony but internet-related data too; (b) an improved infrastructure enabling acquisition of data as it transits the UK, where necessary; (c) business change and training in law enforcement agencies to make use of new data in criminal investigations; (d) some horizon scanning and experimentation, and I would emphasise that is a small amount, to understand continued technical change and future
stakeholder requirements to manage risk; and (e) the setting up of a body to sustain the capabilities of the CCD comms data programme after our build programme has terminated.

Q74 Dr Huppert: So if it turned out that you could not get the agreements you wanted and you need to do more DPI-type data collection, the costs would go up significantly from this £1.8 billion, presumably.

Charles Farr: No, I think—

Dr Huppert: So the £1.8 billion assumes doing a lot of DPI.

Charles Farr: The £1.8 billion assumes doing a certain amount of DPI, but not that DPI is central to this proposal.

Richard Alcock: The majority of the costs are around data retention. Over 50% of the costs are associated with working with communications service providers in the UK and overseas, to establish data retention stores, build on the very good practice that we have at the present time and put in place the infrastructure to secure the access of that information from law enforcement. The costings reflect our strategy, which is that we will spend more on data retention, and that, indeed, is what the focus of the programme is.

Q75 Dr Huppert: Just so that I am clear, an overseas-based company that agreed to store this data for you—Google, Facebook, whoever it may be—you would pay the costs that they tell you they have for doing that; is that right?

Richard Alcock: Not that they tell us. We would work with the communications provider to establish what we needed them to collect in addition to that which may already be retained. What we would be seeking to do is just pay the difference between that which they currently are or may be retaining and that which we may want them to retain.

Dr Huppert: I suspect they will have an interest in trying to inflate that cost, but you will fundamentally be paying overseas companies.

Richard Alcock: It would be audited.

Q76 Dr Huppert: Can I then turn to the flipside—I am rushing through this somewhat; I apologise—which is the benefits? There is a section in the information that was provided that had very little information about benefits and came up with a figure of up to £6 billion, I think it was, over 10 years. Where does that figure of £6 billion come from, and can you evidence it?

Charles Farr: The answer to both of those questions is it comes from us, validated by the Treasury and our own economists. How do we validate it? If I can briefly take you through the methodology, you can make your own judgment.

The benefits assessment was taken from a sample of 13 stakeholders across the user community, including those stakeholders making the most use of communications data. We began with a survey for them of the likely trajectory of communications and communications industry, informed by our own work and, indeed, by Ofcom. We then asked them for an estimate of how communications data was helping the resolution of crime and the protection of vulnerable people now, and their view about how it was likely to do so in the future. We then attached a monetary value to lives saved and obviously an estimate of revenue recovered. The monetary value for lives saved was based on an existing calculation in that regard made by Home Office economists, used for wider purposes in crime work. We can give you the reference of the relevant documentation and, indeed, provide you with copies of it, but it does
attach an economic value. We then made the required calculation. I should emphasise that that net benefit is the benefit deriving from those 13 stakeholders only, not a nationwide survey of all users of communications data. Moreover, the financial value of the benefit does not take account of any financial value that you could put on a murder, because we could not find a sensible, credible, decent way of doing that, nor on a terrorist incident.

In our judgment, the methodology is sound. It was endorsed by Home Office economists. It went to the Treasury. It was in line with Treasury guidance on investment appraisal but, in fact, it does not capture the totality of benefits, because it was based on a survey of 13 organisations and it does not monetise some key benefits for which monetary value was hard to attach.

Q77 Dr Huppert: While prediction is always hard to do, and I totally accept that all of these things are, to some extent, estimates, presumably, given that you currently have 75% of the data that you would want and you are trying to go up to, let us say, 90%, because it will not be 100%—

Richard Alcock: We said 85% earlier.

Dr Huppert: 85%, fine, so that makes the case even easier. Then you are saying there should be benefits of £600 million a year times 7.5 that you can already evidence for the last year. So, presumably, you would be able to supply this Committee with an estimate of the calculation that shows whatever that comes to, £4 billion a year or so, in the last year that was saved or the net benefit as a result of the communications data that we had access to.

Richard Alcock: The benefits calculation is about, essentially, trying to quantify, in monetary terms, that which could be accrued should the Bill be passed.

Dr Huppert: My point is that the communications data you already have, you will know the benefits we accrued last year from that and, presumably, if your methodology works, you should be able to point to where some of that lies.

Richard Alcock: That presupposes we have all the data that is required. We will take that away and have a look at it.

Q78 Dr Huppert: I think that would be helpful. One last question, if I may, Lord Chairman; sorry to presume on this. A lot of the costings and the work rely on this close relationship with the CSPs. I apologise if this has already been asked, but you, presumably, have been working quite closely with the major CSPs; I will not ask for a list of everybody you have spoken to, but I expect we can guess who the major ones would be. In your view, are they all happy with the Bill as it currently is?

Charles Farr: We have referred to that earlier, but perhaps I may repeat what we said. You are right, of course. As you well know, we work not with every CSP but with the major CSPs who are of primary concern to us. We have a good, collaborative and, I believe, constructive relationship with those CSPs, who, I believe, recognise that they have legal obligations and other obligations to provide data in certain circumstances: where it saves lives and helps us convict criminals and protect innocent people. They also completely understand that a gap is emerging between the data that they have and the data that we require. They are saying to us, very clearly, in terms, that they would expect legislation to provide a means for narrowing that gap and that if the legislation so provides, they will work with us to help us to do that.
Dr Huppert: So if we asked them the direct question “Are you happy with this Bill?” when a range of these people come before us—

Charles Farr: I cannot tell you whether they are happy with it. I can tell you what they tell us—and I emphasise I am not talking about every CSP; you can doubtless find one that will have a problem with this—which is that the major CSPs understand the problem that we are trying to solve, understand the technology and the way in which we are proposing to solve it, agree that that technology is feasible and are looking for legislation to underpin collaboration in the future. Whether that means happy or not, I hesitate to say.

The Chairman: Before I ask some other colleagues to participate, could I stress that the Committee would like, then, to get a paper on the historical data of how many lives saved, children safeguarded and money recovered, which would help us come to a conclusion on whether the extrapolated data or the plans for the next 10 years are optimistic or not. And I think we would like the figures from your economist on what is your standard estimate for a life saved or a child safeguarded.

Charles Farr: If I may, the second request, of course, is well understood and we can provide the paper, which was done by the Home Office economist. On the first, we had a similar conversation before. Acquiring that data retrospectively is not straightforward and we will have to look and see what we can do, talking to all the stakeholders about the evidence for that in the past as well as the evidence going forward.

The Chairman: I presume we may put this to HMRC when we see them and we will have the HMRC—

Charles Farr: In some ways, the figures for HMRC are easier to come by, because the financial benefits are easily understandable.

Michael Ellis: Mr Farr, as far as the impact that would follow should the period for which the data should be retained be reduced, could you say something about the effect of that if the Bill was to be altered to reduce it from 12 months?

Charles Farr: I know that you will want to discuss that with the police, so, if I may, because it is more central to our role and my own background, let me say that removing, if one chose to do so, a retention period of a year and reducing that to, say, less than six months would have a significant and serious impact on our ability to investigate terrorism. That is true for terrorism, in particular, because it is often long in the planning and one has to go back to the beginning of the plot to understand, with certainty, who has been involved with it at every step of the way, not only in this country, but overseas as well, because remember, data shows us international connections as well as domestic ones.

Michael Ellis: So you would consider a period of less than 12 months to be untenable as far as the investigation of terrorist offences is concerned.

Charles Farr: Obviously, you will talk to the police and the ISC may talk to the agencies. I think it would be very challenging for the investigation of certain crimes, in particular terrorism.

Stephen Mosley: Clause 1 gives the Secretary of State strong powers in order to specify which communications service providers need to keep the data and, also, to specify what technology they should use. I know that most of them are broadly happy, but what happens if
you specify something and the service provider says, “No, there is a better way of doing it”? Is there any sort of right of appeal or is it a general situation that you would negotiate on an individual basis? Are you looking at standardised technology?

Moving on a bit from that, without asking for specifics, because I can fully understand why you would not want to give specifics, have you got any idea of the general number of CSPs you would be looking at? Are you just looking at public network providers or will you also be looking at private networks, which of course moves us on to the big issue of last summer, which is BlackBerry Messenger? Will that be included?

**Charles Farr:** On your two questions, let me have a go at the first and then perhaps Richard or Peter can talk more competently than me on the second. I emphasise that it is exactly the purpose of this legislation to facilitate a dialogue with industry about the best way to address some of the problems that we have. I have no doubt that some CSPs will have much better ideas about how to address these problems than will we and our technical colleagues and others, and there must be a conversation. I believe firmly that the groups and the relationships we have set up over the past few years to deal with all manner of issues to do with data and interception will facilitate that process and provide for it.

On the second issue, if I may, I will turn to Richard.

**Richard Alcock:** In terms of the general number of CSPs, just in the United Kingdom, I think it is in the order of 250 to 300 communications service providers. We certainly do not envisage working with that many within the piece. Clearly, it depends how communications services change over time and whether groups gravitate to a certain service or not. But we certainly do not envisage working with everyone, and I estimate it will be a relatively small proportion of those.

**Peter Hill:** It may just be worth mentioning that although we do not envisage getting into dispute or confrontation with any CSP about the notice that we would serve on them, there is, as you probably know, an arbitration body, which was set up to deal with interception and is, under this legislation, going to have its remit extended to communications data. That brings together the industry and the public authorities to arbitrate a disagreement over a particular notice and then to make recommendations to the Secretary of State about whether that notice should be maintained, modified or removed. So there is an ultimate route of mutually consensual arbitration.

**Q83 Stephen Mosley:** In terms of private networks, we are thinking in terms of the internet here: internal private company networks, the internal government network, and BlackBerry Messenger. Would they be included?

**Richard Alcock:** We cannot talk about individual providers, but the Bill does enable notices to be served on both public and private networks.

**Q84 Mr Brown:** Can I ask about the use of warrants rather than the use of a more senior official to give consents for data searches? Where local authorities are seeking data they are being asked to go and see the magistrate. Why did you do it one way for local authorities but have a different route for the internal workings of the state?

**Charles Farr:** The Government, at the time of the Protection of Freedoms legislation, took the view that confidence in the authorisation process for seeking access to communications data within a local authority had been damaged by events which you will be very well aware of and
which have been subject to media reporting, and that that authorisation process should be changed and that, therefore, a magistrate’s approval was appropriate. Similar concerns had not been expressed about the authorisation process in the police and had not emerged in quite the same way in the Interception of Communications Commissioner’s report on these matters. Moreover, there is a practical, significant problem that local authority requests for communications data constitute about 0.3% of the whole; police requests constitute, with the security services, 99%. So there is a volume, practicality and logistics aspect involved in moving the bulk of communications data requests across to the magistrates’ warrant system.

Q85 Mr Brown: I appreciate the practical point, but can I put two what seem to me possible snags to you? When searching for an appropriate magistrate, people always seem to find the one who will give them the answer they want rather than the one who might take a more robust and independent view. How strong a safeguard is that? Secondly, where the senior officer may be working day to day with a more junior officer, giving the authorisation, is there not a danger that there will be familiarity and a canteen culture and that people will give the approval too easily?

Charles Farr: On the first point, I recognise the potential problem. Of course, we are only beginning to roll out magistrates’ authorisation for local authority requests and I think we probably have to see how it goes and then come to a judgment. I am sure the Interception of Communications Commissioner will come to a judgment on that as well.

Q86 Mr Brown: That does not really make it a very robust safeguard. What is the magistrate’s function?

Charles Farr: I think my point is it remains to be seen. It is a response to concerns which have been expressed about internal authorisations and the specific environment of local authorities and incidents that had taken place connected to applications for communications data. I think a magistrate will impose greater discipline on that process. The Government has not seen the need to do that for other public authorities. We will have to see, I think in the commissioner’s report, how effective it is going to be with local authorities. It is too early to say yet; the process has not begun.

If I may, I will ask Peter to comment on your second question, which is whether, as I see it, a sort of informal network in other public authorities may facilitate, in an unhealthy way, applications for communications data.

Q87 Mr Brown: We are all human. Where is the safeguard?

Peter Hill: It lies in the authorisation process. So, firstly, I think sometimes there is an idea that there is a police officer sitting at a computer terminal who can access communications data when they like. That is not how the system works. There are a small number across the country of accredited, trained, identified single points of contact. By “identified”, I mean they have a unique PIN number which allows them access to the system, so it is not the question that anyone can log on and pull off this data.

The person authorising it at the senior level should be unconnected to the investigation. So there will be an investigator saying, “I think communications data might be useful in this process”. They will go to the specialist and say, “What sort of data might I be able to get?” Together, they will come up with an application. The senior officer will then say,
“Do I agree that it is necessary and proportionate?” and then the specialist, the single point of contact, will issue the authorisation, log on to the system and get the data, so there are a number of people involved in that process, overseen by a senior responsible owner in the police authority. Of course, that process produces the audit logs. Those are inspected by the Interception of Communications Commissioner. He reports on the use that the police and everyone else makes of those powers. In the end, many of these cases end up in court, so the communications data will then be subject to the normal processes.

It is a rather long answer, I am afraid, but it is useful, I think, to know what the internal authorisation process is within the police to understand that it is not simply a question of somebody sitting at their desk, their mate next door asking for some data, and them logging on and pulling it off.

Q88 Mr Brown: I think it is helpful to us to have that explained in the way that you just have done.

Charles Farr: I just wanted to reinforce the point—and I apologise for the obscure language—about the single point of contact inside the police, who, as Peter has said, is there both to offer technical advice to the applicant—the person running the investigation who thinks they need communications data—and to facilitate access when approval is granted. The single point of contact is someone whom we are responsible for providing training programmes for and whose training and security we take extremely seriously, as, indeed, do the police. It is not a casual appointment and a casual part of someone’s career in the police. I hope, when you talk to the police, that you are able to get from them a sense of what the SPOC, so-called, means and does, and that will reassure you about the thoroughness with which that role is approached by people who are in it.

Q89 Mr Brown: Has any information that you have obtained so far been improperly released by people who should not have released it, and have they been caught and prosecuted for so doing?

Charles Farr: The Interception of Communications Commissioner’s report is due out on Friday. I hesitate to pre-empt what he may say on this, but of course it is part of his job to look at instances where the system has not behaved in a way that it is intended to do.

Q90 Mr Brown: On the prosecution point, how often was the offence of misconduct in public office prosecuted last year?

Charles Farr: In general?

Mr Brown: It is almost always about a public official obtaining information and selling it on, usually, but not always, to a newspaper, maybe working through a private detective and then using it, usually, for selling newspapers.

Charles Farr: Peter may have the statistics, but, as you know, there are a number of investigations under way at present, which are adjacent to this.

Q91 Mr Brown: You can see why this would be at the forefront of the public’s mind.

Charles Farr: I can understand that, yes.

Peter Hill: All I can say is that in the reports that I am sure you will have seen, and you will see when the latest report is issued in the next few days, there have been, so far, no occasions
when Sir Paul Kennedy, the inspector, has identified what one might call wilful or reckless errors or releases of data. Of course, as in any system, there are errors, but what I think you are talking about is either something that is wilful, reckless or criminal and, so far, the inspection regime in relation to communications data—and I hasten to add that this is in relations to communications data—has not identified such cases.

Q92 Mr Brown: If caught, what would you say to me to convince me that somebody who had done such a thing would be robustly punished? Under what offence would they be prosecuted?

Peter Hill: There are, as I am sure you know, a number of offences on the statute book. Under the Computer Misuse Act, it is possible to prosecute people; there are custodial offences there, for a number of years. If it is a data protection offence, there are the offences in the Data Protection Act.

Charles Farr: Currently under review, of course, in relation to Section 55.

Peter Hill: Yes, and of course there are the misconduct in a public office offences, which carry, potentially, extremely serious custodial sentences.

Q93 The Chairman: There is nothing on the face of this Bill to reassure the public that any abuse of power from a police officer or any other officer or designated person will be treated very seriously. Why not put some criminal sanctions in the Bill?

Peter Hill: We can certainly take that away.

The Chairman: We look forward to Sir Paul’s latest report. It just seemed to me, reading the 2010 one, where 94% were performing satisfactorily or were good, one wonders what the other 6% were like, or that 44 police forces were up to speed, but two were very poor in the way they treated data. It just seems to me that the sanctions in those cases were about a bit more training and a bit more advice, whereas if there was the possibility of a criminal penalty there, whether or not it was used, it might reassure the public. I am sorry, Mr Brown.

Mr Brown: I happy to leave it there for now, but I think we should return to this and there is a doubt in my mind as to whether the criminal sanctions work.

The Chairman: If you have any further advice to give us on criminal sanctions, we will happily receive a paper on it, but we will wish to return to this, as Mr Brown said.

Q94 Stephen Mosley: There is one big difference with this Bill: Clauses 14 to 16 establish a request filter, which seems to me to be an incredibly powerful tool. It will allow the people who are accessing the data to basically scan all of these individual databases and bring the results into one place; it will be a very powerful tool. It will be operated, as I understand, it says, by the Home Office. What sort of checks and balances will be on this new tool? How will it work?

Charles Farr: The Interception of Communications Commissioner’s powers are, of course, being extended with specific reference to the request filter. There will be very detailed audit logs indicating exactly what requests have been made, what results have been produced and, of course, an examination and confirmation of the fact that extraneous data has been destroyed and never makes it to the public authority in what is an automated process. So there is quite a lot of reassurance built around new oversight bodies plus new automation plus new audit controls.
On ownership, I think Ministers certainly envisage that a tool of this kind must be operated by a public authority. It is possible that, as the NCA builds, that might provide a home for a capability of this kind, but I think until such time as it has, it is premature to make a clear conclusion beyond saying, of course, that a public authority will own and operate this—at present, the Home Office.

**Peter Hill:** I think you used the word “databases”. Just to be clear, the filter only relates to accessing communications data. So a request will be made, for example, to know who the subscriber to an e-mail was, or “This phone was in these locations”, and it will take that communications data. First of all, it will tell the person asking how much data is likely to be necessary to answer that query, so it will help them make the judgment about necessity and proportionality. If they go ahead, it will then sift out the irrelevant data and give them the relevant data, not the data they do not need. I entirely take the point that it is a tool that can do a lot of things, but the point that this is a safeguard to try to focus the data that is being asked for is an important one. Rather than getting all the data and then sorting it within a police authority in order to get the bits you need, having a process which does that without human involvement should reduce the data that is being disclosed, not increase it.

**Stephen Mosley:** So, effectively, it will interrogate the communications data that is held by the third parties and bring the results to one place.

**Richard Alcock:** Yes, on a request-by-request basis.

**Q95 Lord Armstrong of Ilminster:** I think the legislation says that things would be authorised by senior designated officers, and that those officers would be defined in negative orders before Parliament. I think there are two things on this. First of all, I believe that in the police the usual rank is superintendent, and I wonder whether superintendents are not a bit too close to the coalface and the operation, and therefore whether it should not be a chief officer who is required to give authorisation.

Secondly, is it is good enough for the senior designated officer to be labelled by a negative order? Should Parliament have slightly more say in how that is applied, not just in the police but in other services or authorities?

**Charles Farr:** Perhaps I can take the first of those two questions and Peter can deal with the second, on the negative order. I think there is, as you have realised and seen, a set of serious issues around the appropriate level for a senior designated officer. The police will doubtless comment on this, if you ask them. I think there obviously is a case for pushing up that level to a senior ACPO-level person. We looked at that, and Ministers were persuaded that that was not necessarily appropriate, because a superintendent perhaps has a closer feel for the day-to-day operations and, therefore, has a better sense of necessity and proportionality, probably has more time to devote to a particular application and, critically, of course, is still separate from the investigation. As in Peter’s answer to the earlier question, they must not be a part of that investigation and can remain detached for it. For all those reasons, Ministers were persuaded that a superintendent remained the right level, rather than pushing it up to an ACC or a DCC at ACPO level. However, there are clearly alternative views and you will, I am sure, ask the police about that.

Can we address the second issue?
Peter Hill: On the second, I need to go back and check, but my understanding is that the order that sets the authorities, the purposes and the approvals levels is by affirmative procedure, not negative. We can come back to you and confirm that.

Lord Armstrong of Ilminster: If that is right, that deals with that question.

Charles Farr: We will check that.

Q96 The Chairman: Finally, Mr Farr, I think you have said that the driving force behind this Bill was voluntary collaboration and co-operation with the CSPs. You have had informal assurances or verbal assurances from them. Have you had anything in writing from chief executive officers of some of the big CSPs that they will play ball?

Charles Farr: Richard may be able to correct me, but we have not sought anything. I do not think we would intend to do so. That would look, I think, less than collaborative. Our Ministers have talked to senior office holders in those companies, and I think we have received the assurances that we would expect.

The Chairman: “My word is my bond”, yes.

Baroness Cohen of Pimlico: You do not need civility if you have legislation.

The Chairman: Thank you very much, gentlemen. It has been a long session, but this was a very important opening session. It has been much longer than I expected, but we are determined, in this Committee, to be very thorough in every session. By the time we report we hope we will have looked at absolutely every aspect of the Bill and the proposed legislation. Thank you all very much.
WEDNESDAY 11 JULY 2012

Members present:

Lord Blencathra (Chairman)
Baroness Cohen of Pimlico
Lord Faulks
Lord Jones
Lord Strasburger
Mr Nicholas Brown
Michael Ellis
Dr Julian Huppert
Stephen Mosley
Craig Whittaker
David Wright

Mr David Davis MP, Big Brother Watch [Nick Pickles], Open Rights Group [Jim Killock] and Privacy international [Dr Gus Hosein] (QQ 97-126)

Examination of Witnesses

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

Q97 The Chairman: Welcome to our second evidence session. We are starting about a minute early because we have some rather difficult time constraints today. I say, for the benefit of the public in particular, that we have had to cancel our second evidence session. It is likely that possibly from 3.30 onwards—although hopefully slightly later, if we are lucky—there will be a series of votes in the Commons. That would cause disruption of 15-minute intervals on maybe four or five, or even up to eight occasions. It would make a mockery of trying to hold the second evidence session. We will crack on as briskly as we possibly can with the first evidence session. Welcome, Mr Davis, Member of Parliament, Mr Pickles, Mr Killock and Dr Hosein. Perhaps we could begin with each of you just saying who you are, for the record.

Mr Davis: David Davis, government Back Bencher.
Nick Pickles: Nick Pickles, Director of Big Brother Watch.
Jim Killock: Jim Killock, the Executive Director of the Open Rights Group.
Dr Hosein: Gus Hosein, Executive Director, Privacy International.

Q98 The Chairman: Excellent. Thank you very much. Gentlemen, could you each start by outlining briefly your main concerns about the proposals embodied in the Draft Communications Data Bill? What are the areas you each hope that this Joint Committee will consider, and who are the main witnesses you think we should hear from after yourselves? Mr Davis?

Mr Davis: Can I start slightly backwards, Lord Chairman? I start from the position that the RIPA arrangements we currently have, before we put this new procedure in place, are too lax.
When they were put in, I think in 2000, the arrangement they replaced was a combination of voluntary and warranted arrangements, which I think were much safer than we currently have. In essence, what I see as the current problems of the RIPA arrangements on communications data are similar to those that will be reflected in the current proposals. I think a warrant arrangement would be a generally good idea on both sets of legislation, helped, of course, with some accelerated procedures, which we can talk about as you go through questions, no doubt.

I have concerns about the security of the retentions that are now being required under the new law. I think that will create a huge security problem, not with the Government but for individuals and the private sector. I have some concerns too, bluntly, about the quality of evidence put out by the Government. Because we are in essence dealing with agencies that are relatively confidential in their operations, it is very, very difficult to get down to how effective their current operations are, and the extent to which they are simply using our blindness to extend their capabilities. I can give you examples of that by parallel with other bits of legislation, if you wish.

I have some concerns about the technical competence of the proposals being brought up, but I think other members of the panel will give some views on that. In terms of where to look, there are some very obvious things that will come out. I will not give you a long list, but there is one that strikes me as being unusual, which might be worth looking at. It is that the German state recently struck down the parallel arrangements for our RIPA operations—which, again, I say are like a metaphor for this—and as such we can see how effective policing and security operations were in that state when they had a RIPA arrangement, and when they did not have it thereafter. I think the policing improved across that.

In terms of witnesses, there was a German Member of Parliament, called Malte Spitz, who asked about the information kept on himself. I think what he found would be very interesting to you, but just as a possible witness. The other thing I would look at, if I were in the Committee’s shoes, is not just the direct impact of this, but international agreements that apply to it. What data will be collected under these arrangements that will be available to other states under our existing agreements, particularly European but others as well? I think you will find they are pretty intrusive.

Q99 The Chairman: Thank you very much. Mr Pickles?

Nick Pickles: I start in a similar position. This has been presented on the premise that it is maintaining an existing capability. I think the Committee should look very closely at the validity and the honesty of that statement. We are going from an environment of fixed communications, where people had a landline phone but did not carry mobiles, where the internet was not pervasive, and accordingly the colour of data available was very different. I think it was actually made in evidence in 2009: this is a far more colourful capability, which allows the state to look into far more detail of your life than was ever possible, whether or not that is the websites you visit; we were never previously required to declare the newspapers that we read, but that will now be possible under this. The actual credibility of saying that this is not a new capability, I think, should be looked at.

This is unparalleled on an international scale. Find another democratic state that wants to record this level of detail. Indeed, one witness I hope will be able to give evidence is the Foreign Secretary, because it appears that this is at odds with a substantial proportion of what
is currently British foreign policy. If you listen to the remarks of the Foreign Secretary in the
cyber conference in November, he talks about privacy as being an essential part of the
internet, and the Vice President of the United States went on to say that where countries
pursued monitoring arrangements, that would likely lead to businesses moving abroad to
avoid those monitoring arrangements. I hope that will be looked at in terms of a serious issue
for British reputation.
I share David Davis’s concern that the evidence we have heard so far has been scant and
indeed, if you consider that this proposal has been formulated for several years now, that the
last consultation was in 2009, that there are currently 120 members of staff working on this
directive in the Home Office, the number of times this Committee was told yesterday, “We are
working on getting the data, we do not have the information,” was quite surprising. I hope
that the evidence of effectiveness is brought to bear.
I think the filtering provisions, again, as we heard yesterday, warrant extremely close scrutiny.
It is quite disingenuous, indeed, to suggest that this is not a central database merely because
there are lots of little databases. If you connect all the little databases together you have by
proxy a central database, and one of the concerns I have is that the filtering provisions open
the door for fishing trips to find out who was in a certain area, things that are not currently
possible. Again, that is a new capability.
Finally, one essential part of this inquiry should be the police forces of England and Wales,
who are currently struggling to deal with the laptops and the phones that they recover at
existing crime scenes. This resource will divert from their capability to deal with evidence they
are already gathering. We must make sure the police are not unduly penalised, and I am sure
colleagues will have more points to make on that.

Q100 The Chairman: Thank you very much. Mr Killock?
Jim Killock: Thank you. Picking up on Nick’s point about observations back in 2009, the EU
Council of Ministers talked about a “tsunami of data” hitting the police, and welcomed that
opportunity, commenting, “Every object the individual uses, every transaction they make and
almost everywhere they go will create a detailed digital record. This will generate a wealth of
information for public security organisations, and create huge opportunities for more effective
and productive public security effort.” Those are the words of the European Council looking
at the pattern of data that is emerging in the digital age. I think that is where the focus of this
legislation should be. It should be looking at the amount of data that is going to be available to
the police and law enforcement in the future, as a result of the digital tracks that we create,
and how access to that is then regulated. I think that presents a hugely different picture from
the one presented by Charles Farr yesterday of a declining availability of data. The fact is that
data is proliferating. There will be about 1,000 times more data available over the next decade,
just because of the increases in capacity for storing data through digital technology.
On the question of communications data itself and the sort of data sets that Charles Farr
believes are becoming inaccessible, despite the fact that those are probably proliferating in
terms of communications events that are recorded, I think it is worth investigating the
potential routes that are currently available to gain access to that data. There are legal routes
within this country; there are legal routes abroad, in Europe or America or other countries
where we have co-operative agreements between the police here and abroad; there are
possibilities of intercepting that data within the UK. We have intercept capabilities across
ISPs, and we also have the possibility of seizure of devices. If a device has recorded the communications events that an individual suspect has engaged in, then those devices can be seized and they can be examined. The number of cases where communications data may not be available, it seems to me, are likely to be rather small. It is good piece of work for this Committee to engage in to try to ascertain that.

Another piece of work the Committee should be looking at is exactly what the current position is with retained data in European law. The data retention directive has been challenged successfully in a number of European states. It has been declared unconstitutional in a number of countries. Currently, as David Davis mentioned, it is not in operation in Germany for this reason. The Committee should try to ascertain whether it is actually compatible with the European Convention on Human Rights.

A little bit more broadly, we should think about the change that is being suggested in this Bill. We have moved from a question of police access to communications data, which was the traditional position with telephone records, to retention under the data retention directive—that is to say, you keep it for longer under obligations in law—to a question of collection of data. That is a fundamental shift in approach, and it deserves a wider debate, as does the question of data mining, which may flow from creating the ability to query these databases or datasets mentioned in the filtering arrangements. What are the implications of data mining? What sort of information might emerge from that? What are the security and cost implications that flow from this entire arrangement?

Moving on to the question of witnesses, I would start off by asking: “Where has the consultation process been?” The Committee should establish exactly what the consultation arrangements for this Bill have been. I think all of us, as witnesses, are struggling because we do not have a proposal. We do not have a set of evidence that says why this must take place. We do not have a firm proposal outlining how this will operate. All we have is the legislation, which should come after both the evidence and the proposal, to allow the Government to take on the duties that it has identified it must take on—

**Q101 The Chairman:** Can I interrupt you there, Mr Killock? I am conscious you are in full flow, but we are on a very tight timescale.

**Jim Killock:** Of course. My last couple of points: the Article 29 Working Group I think have been looking at data retention very closely. Perhaps invite Digital Rights Ireland, who have experience of abuses of retained data in Ireland and of bringing cases on human rights grounds to the European Court of Justice. Involve overseas communications service providers, because they have a very different view of the legal compulsion surrounding them from the one presented by the Home Office yesterday.

**Q102 The Chairman:** Thank you. Dr Hosein?

**Dr Hosein:** I will restrict myself to two points, because my colleagues have done such a great job already. One quick preface: as an academic and as an advocate, I have followed communications surveillance in this country since 1997. I have been here for all the key debates about encryption. I was here when the debates took place on RIPA and on the Anti-terrorism, Crime and Security Act. I was at the European Parliament when data retention went through, and I have been following this specific policy since 2006-07.
Having said that, my first concern is that I still have no idea what this policy calls for. Until we see the draft orders, we have no idea what will be asked of organisations. We have no idea what a third-party provider, say, in California will be ordered to do. We do not know what the nature of the black boxes is, if there are black boxes, how they will be implemented at providers in this country, which black boxes, or what they will actually collect. I do not know when that debate takes place. It is hard for me to identify problems with the Bill when I am still not entirely sure what the policy is.

The second component, as much as I have been able to identify the issues involved, is a sea change around collection. That is, the settlement at a technological, economic and just at a political level over the past 15 years, if not the past 35 years, has been that telephone companies collect this information for their business purposes. It exists within logs. Once that information exists within logs, it can be accessed. It can be accessed lawfully by organisations. That has never been contested. The quality of the access has always been contested, but that is fine. Over the past 15 years, through debates in Parliament about communications surveillance, it has always been about regulating access.

Now what is being introduced is the notion of collection. Organisations that have no business purpose to collect information will be asked to collect this information solely for the purpose of some future potential access, because one of their many consumers may be relevant to an investigation down the road. That is the reason why this policy has never been taken up in a democratic country: that sea change of requiring collection where there is no business purpose originally.

The Chairman: Thank you very much. Thank you, gentlemen; that is very helpful.

Q103 Lord Jones: Lord Chairman, gentlemen, the question at the moment is the present law relating to the retention and acquisition of communications data, and we would like, please to hear your views. Does it broadly achieve the correct balance between the need for law enforcement and national security, a big priority, to access communications data, and then an individual’s right to privacy? We would like to hear your views about where the balance should be, between the individual, who has rights—it is all about liberty and privacy—and the need for our nation to be secure and not to be the victim of terrorism. What is your view? What should be the balance?

Mr Davis: Shall I kick off? The first thing to reiterate, which has already been said, is that we are rather hard-up for some aspects of information on this. We do not know how many things have been turned down, how successful each individual request is, and so on. However, the sheer numbers—we have 550,000 or so access requests per year—seem an awful lot of data. We can come back to what it really means in a minute.

The accelerated access requests—and we are just talking 2010 data—is 31,000, up from 21,000 the year before. I cannot think that there were 50% more kidnaps, or 50% more terrorist events, the sorts of things that ought to perhaps precipitate an accelerated request. My hunch, and I cannot put this stronger than that, is that what is happening is that the agencies are, quite understandably, using every power they have without any thought of restraint. I suspect we will find when we investigate this, if we can, that a great deal of that information is wasted, a great deal of it is unnecessary, and as a result it is an unnecessary intrusion on an individual’s privacy.
Q104 **Lord Jones:** Anyone else?

**Nick Pickles:** I think we do not have the evidence. We know there are more than 550,000 requests, but is there any evidence offered as to how many of those are terrorism-related? We are told the information is in progress. It is remarkable that I managed to get, through the freedom of information law, more information than the Home Office team yesterday seemed to have, but one police force did give us a breakdown of why they were using communication data by offence type, which I know is something that was discussed yesterday. Traffic offences is on that. Terrorism is not. Humberside Police—

**Mr Davis:** My police force.

**Nick Pickles:** —confirm that they have used it nearly 200 times in three years for traffic offences, and terrorism is not listed as one of the crimes. They even beautifully list the category “other non-crime”. I am happy to make this information available for the Committee. Let us look at the numbers: in Germany they did. They went through, when this was being debated, and the German Federal Criminal Police Office looked at 381 cases where communications data was cited as critical, and of those 381 cases, two had a link to terrorism. I want to see the Home Office bring forward the same evidence. Why are we sitting here discussing this, saying, “There are lots of terrorist cases, but we do not know how many”? It must be very difficult to manage your investigations if you do not know how many investigations you are currently running. I think the position has been presented from the start as, “We need this information,” and when we ask why, we are told, “We cannot tell you.” For the unprecedented scope of these proposals, I am sorry but that is not good enough. This is bringing to light the fact that every British citizen now carries in their phone a tracking device, and makes that information available. That is unprecedented, and is not currently the case under existing law.

Q105 **The Chairman:** Not every colleague needs to intervene unless you particularly want to. I am conscious of the timescale. Can I ask Dr Hosein?

**Dr Hosein:** If I may take a structural approach to the question you have asked, it is not for us to say yes or no to your question. It is more interesting to ask the question as to who is the one who decides on a case-by-case scenario. Parliament should decide where that balance is struck, but what we have seen is that for the past 12 years Parliament has been relatively unhappy with RIPA, but very few fixes have come along in a 12-year period. Should we leave it to the judiciary? The judiciary is not involved, unlike in other countries where there is usually a court order involved in deciding whether access to the data, on a case-by-case basis, is relevant. Is there some independent regulator, as there is in some countries? No, there is not. Who has to make that balance calculation? It is the police. That is not the way it is done in democratic societies. That is not how it is done in accordance with Article 8. You need to come up with a system for deciding on a case-by-case basis what is necessary, what is appropriate, what is proportionate. It is an interesting debate for us to be having, but 12 years into RIPA we should be asking: “On a case-by-case basis, where should that question be asked, and who should be answering it?”

**Nick Pickles:** One brief point on that, which was again on the figures, to use one example of Kent Police: in two years they made 7,664 requests for communications data. Within the police force itself they ruled that more than 3,000 were inappropriate. There are a lot of police officers making mistakes about the proportionality of using this capability.
**Q106 The Chairman:** I think we would like to see that data.

**Nick Pickles:** We are currently working through about half the police forces, but I am more than happy to share it.

**The Chairman:** When it is complete we would like to see it.

**Nick Pickles:** There are only three staff in Big Brother Watch, unfortunately.

**Q107 David Wright:** Mr Killock, your line earlier was that there is “significant data proliferation”. I think all of you would accept that. Charles Farr and the other members of the Home Office team yesterday were talking to us about this gap, about the fact that they wanted to put in legislation that would bridge their capability gap and draw them up to, I think, 85% of accessibility. You have made a good series of introductory points, but my concern is that there will be this gap. We can argue about thousands of bits of data, but what about the two that sneak through, which we could have identified, which relate to terrorism? What we have to do, as a Committee looking at this Bill, is to get the balance right between exploring the data gap that we are being told about and making sure it is targeted properly. Do you accept that there is this gap, and we do need to make it up?

**Mr Davis:** It is an oblique answer, but I will draw your attention to the 7/7 bombings. We missed them. Did we miss them because we did not have data on them? No, we did not. We missed them because we had 2,000-plus targets, and we misclassified them. This is not the only examples of the agencies screwing up—not to put too fine a point on it—because they have a large amount of data that they do not know how to manage. You could even, if you have them in in private session, ask them about the effectiveness of their data management systems. I can tell you, they had to use the Cabinet Office’s data management system at one point. You have two problems here. One is the availability of the data; the other is the manageability of the data. Do you improve the effectiveness of your crime-fighting by gathering data on 40 million innocent people?

**Q108 David Wright:** The point that the Home Office are making is that yes, you do. That is clearly the pitch we were being given yesterday, that yes, it does.

**Mr Davis:** The evidence is the other way. You need to talk to them about actual operations, to show how many times they make mistakes that arise directly out of misclassification of the data. The famous line has been used: “They are looking for a pin, and they are creating a field full of haystacks.”

**Jim Killock:** Just a little bit of information there. David Davis mentioned what had happened in Germany. In both Germany and the Czech Republic, when they stopped having access to communications data under data retention, their rates of solving crime went up. In the Czech Republic they had a tenfold drop in the request for data, because data retention was ruled unconstitutional, but the rate of solving crime went up from 37.5% to 38.5%. That does not really say that this data is always or even largely critical for law enforcement. What you probably need to do, if you really want an answer to your question, is to drill down very, very carefully in the cases that they are presenting to you, where they have used communications data. You have to forensically ask in each case, “Was that critical to solving the crime, or would they, or could they, have found the same individuals through other parts of data or
other parts of the investigation?” Generally, I think, communications data can be useful, but it is probably not always critical. That is something you need to investigate, I would suggest.

Mr Davis: Case-by-case, I am afraid.

Q109 Dr Huppert: Before I ask my question, could I declare an interest as a member of the Advisory Council of the Open Rights Group? You have all been quite clear, I think, that there is a lack of clarity about what is being requested. To me there are two issues. One is what the Home Office currently plans to do with an order, and I presume you have spoken to them and asked them what that is. There is also an issue about what the limits of the powers given by legislation for future orders are. Do you have any clarity from talking to CSPs about what the issues are with those two? Is it acceptable, either as the order they intend, or as the order that could come later?

Dr Hosein: It is very difficult to speak about examples, because there is not an order out there that they even point to, but let us use one example that we have heard of, which is that an order will be placed against Google. Google will be required to collect more data on UK users, to then retain the data on UK users, and to disclose data on UK users. The challenge that arises is, first, a lot of these providers do not know what a UK user is. There may not be a field saying, “Yes, I am from the United Kingdom, I have an account,” as often happens in Skype; you do not actually say what your country of origin is.

Then we are paying these companies to collect information on users. These companies are experts at making a great deal of money off the collection of information on users. We tend to fight on a regulatory level to ensure data minimisation among these companies, but here not only will we ask them to collect more information, but we are actually willing to use British taxpayers’ money to pay for them to collect more information. That is what this policy would entail, at least when it comes to these third parties.

For an ISP in this country, we presume it involves an order to require them to install a certain type of technology according to a certain type of spec, of which they may pick one or two options, put them in, and ask no questions. Now of course there is a Technical Advisory Board that may meet to question whether this is the most appropriate technology, but once that technology is in those ISPs, do they have control over that technology? Can they decide what that technology does or does not do? Can they decide when that technology is updated, and what it then grabs? They probably cannot.

Q110 Michael Ellis: I would like to try to pinpoint the issues down a little, if I may, gentlemen. Do not all feel the need to answer each question individually. Many of you have criticised the draft Bill on the issue of authorisation, by which I mean the draft Bill does not require public authorities other than local authorities to seek any independent authorisation to obtain communications data, by which I mean a magistrate or judge or any other type of independent organisation. At the moment, the Bill envisages a senior designated officer from whichever public authority is relevant—I think a superintendent, for example, in the police, or the equivalent—to authorise requests.

Do you think that independent authorisation should be required for every request? If so, would that be practical? We have heard evidence already that there were over half a million requests last year. Or would you find that somewhat expensive and time-consuming, if you had to seek a magistrate’s authorisation 500,000 times per year?
**Mr Davis:** Shall I start? Firstly, the reason it is 500,000-plus times is because you do not have a proper checking procedure. That is the first thing. The second thing is that if you raise the 550,000 in another context, Mr Farr and the Ministers rush to tell you that this is not 550,000 people. Indeed, in one criminal case it could be 1,000.

**Q111 Michael Ellis:** They have already said that.

**Mr Davis:** They have already said that? Of course they have. This has implications for the warrant process. They say for example, if you were murdered, heaven forfend, they would look at your phone record and then look at who was involved. Let us use phones, because it is easy and it is in place already.

**Michael Ellis:** Yes.

**Mr Davis:** Then they check on every single one of those. That is one warrant. That is not a whole series of warrants. You are not talking about 550,000 warrants, just as you are not talking about 550,000 people. The issue that is material here, however, is speed in the individual case. There are circumstances, and I will stick with phones, but it is applicable elsewhere, particularly with kidnap, where location data is used. If I kidnapped Mr Pickles here, and it was an active kidnap—

**Michael Ellis:** There is a need to move quickly.

**Mr Davis:** There is. Under circumstances like that I am perfectly happy with a very accelerated, or even retrospective procedure, although quite a tight one. They are small numbers, however. They ought to be small numbers. As for the rest, frankly, there ought to be a deterrent not to use it frivolously. In that respect, I completely turn over the argument you have put.

**Dr Hosein:** If I may bring up the international angle on this, the United Kingdom stands relatively alone in the democratic world for access under this type of regime. Let me use the United States as an example, because the United States is often picked on for its lax regime: outside the field of national security, when it comes to access to communications data, it requires a court order. Not only does it require a court order, but it also requires, by default, notification to the individual, after the investigation is complete, that their data has been accessed. This is in the United States.

**Michael Ellis:** It is expensive, is it not, though, Dr Hosein, to go through a court order on every occasion?

**Dr Hosein:** I think the Americans see it differently when they say it is according to their constitution.

**Q112 Michael Ellis:** None of you would be concerned about the expense to the public purse of having to go through lawyers and courts every time the police or—

**Jim Killock:** I think the other question about 500,000 requests is that most of them are probably for subscriber data, which is a relatively routine matter. It would be really helpful if the Home Office would make some sort of disclosure around how many of these 500,000 are simply for whose phone it is.

**Q113 Michael Ellis:** I was going to ask about that, actually, Mr Killock, because there are types of data. You allude to subscriber data, which is simply the data to acknowledge the name
of the person who has the subscription. Most would argue it is not as sensitive as some other types of data. Would you be more relaxed about that being obtainable without a warrant?

**Mr Davis:** Slice through the middle of it. I have no need, in my mind, to have a warrant to effectively operate a directory inquiries, which is what this amounts to, giving name and address and some basic details—maybe other phone numbers. However, I would say you would still need a warrant for details about your account funding, where the bank account comes from and that sort of thing.

**Q114 Michael Ellis:** Are there public authorities that you can accept should not have independent authorisation? Would you say that everyone should have authorisation—police, security services, no exceptions?

**Nick Pickles:** I think Gus’s point about the American system is absolutely right. If the FBI want to put a GPS tracking device on a car, they have to go to court.

**Mr Davis:** I think no exceptions, for two reasons. One is that if you look at this 550,000-odd, the vast majority are policing and security agencies. The famous ones, the local authorities and so on that are semi-frivolous, are really quite small numbers. If we are dealing with the issue, the big issue is law enforcement.

**Michael Ellis:** Of course the local authorities now would have to seek independent authorisation.

**Mr Davis:** Yes, of course.

**Q115 Michael Ellis:** Do any of you have any evidence about individuals who have suffered harm as a result of their communications data being accessed by an investigator?

**Mr Davis:** Not in a critical area, but if you had asked us that question about phone hacking by newspapers five years ago, the answer would have been the same.

**Dr Hosein:** As long as you are not notified of the fact that your data has been accessed, you can never know that that was the reason why you were harmed.

**Q116 Michael Ellis:** Is it not right that, for example, for the person who has a supermarket club card, the data that is held on that by the company in question—I just use a supermarket as an example—can be in and of itself really quite extensive? Are you not seeking, by the positions you are taking, to put an extra burden on those who are trying to prevent and solve crime than is put on commercial entities in the operation of their affairs? What do you have to say about that?

**Nick Pickles:** We have spent the past five years, if not more, arguing for greater protection for consumers. One of the main areas where consumers need more protection is where they are not aware their data is being taken. That is a huge problem. However, the broader point is that this 550,000 figure is a very large number, and nobody has quite established why. I think that should be deeply concerning. I know the Home Secretary used the example of a CEOP operation, where you have identified somebody at the centre of something that is criminal, right now, and without any court authorisation that individual’s communications, including content, can be monitored. One question to ask, say, the police would be why in that situation they would rather arrest an individual and then rely on communications data than monitor the individual and, including content, see whom they are communicating with, before they make an arrest.
Mr Davis: Can I just put that number in context, 550,000? In the same year, I think the FBI’s total number of equivalent comms data requests was 17,000, and a maximum over the course of the previous decade was something of the order of 50,000. That puts it in context.

Q117 Michael Ellis: On the issue of the warrants system, are you all satisfied that that would be any more robust than a senior designated officer who would be specifically trained in the area that he or she would be dealing with and would be subject, after all, to criminal sanction if they abused their authority? Would you not be concerned that a system that requires a magistrate’s authorisation or the like is open to abuse as well?

Dr Hosein: That is an excellent question. That is why, in other countries around the world where they already have judicial authorisation, they still have complaints as to what that judge is actually assessing, how much information he or she has to make a decision on whether something is proportionate, and whether they are able to say no, or they just have to do a rubber stamp. These are questions even within countries that have judicial authorisation.

Q118 Michael Ellis: It could go through on the nod?

Dr Hosein: Or to put it better, at least they have judicial authorisation as a starting point, to then deal with the exact same questions that we are dealing with here.

Mr Davis: The reason I have used the phrase “the guy at the next desk”, which of course is apocryphal really, is because I was communicated with by the staff of one of the commissioners involved, at the time of my by-election, who rang me up and said: “Keep going. You are absolutely right, because this is what goes on. People have the same mindset, and they do not challenge each other.” That was his comment. It was not a question of abuse; it was a mindset.

Nick Pickles: I think that mindset is illustrated by the fact that in 2010 there were 30,000 oral requests approved under RIPA. There was never a written-down document asking for permission. It was orally approved. I think that illustrates that culture.

Q119 Michael Ellis: Two final points from me, if I may. Firstly, do you consider that any of this within the Bill would be effectively in breach of the Human Rights Act, if I can raise that? Do you think, for example, that Article 8 is in issue here? Would any of you approve of some half-way house measure, whereby there would be a level of third-party control somewhat short of a full warrant system, but which would have some other mechanism, and how do you think that would work, if any of you are in favour of that?

Mr Davis: On Article 8, you are a better judge than me, sir. On the issue of a half-way house, no. I would look at the question of how big a warrant should be and what it should cover. That would reduce some of the burden involved. I would look at the question of accelerated procedures, which would be used very rigorously, but are the area of importance in my view. None of us, I think, wants to undermine police effectiveness in this. We are much more worried about that than cost, in truth, and I think that is the way to do it: through the warrant structure and the accelerated procedure.

Nick Pickles: I think a straightforward question of civil society is that this is the kind of tracking that China and Iran are quite fond of. Does Britain want to be a country that has that amount of information retained about its citizens? Specifically, you can call that human rights, you can call that decency, you can call that liberty. There is a question over judicial remedy,
particularly with regard to the fact that, in 99 of the 210 cases heard by the Surveillance Commissioner to date, I think, they have resulted in no judgment either way. That is remarkable with any court, to have nearly half the cases with neither one side nor the other winning. I think that is an incredibly broad question as to the half-way house, but I think you have a fair impression from all of us that the situation we are in today is not good, and we need to be moving backwards from that.

Q120 Baroness Cohen of Pimlico: One of the fundamental questions that has struck me, as someone new to this, is that in a way it seems a little odd to have a system that picks up first whether a communication is taking place, and then second the content of that communication. Am I right, Dr Hosein, in thinking that if you applied for a warrant in the States you would apply for both—that the communication was taking place, and what it was saying?

Dr Hosein: Based on the cases that have hit the Supreme Court, the police decide what will be the most effective measure based on the evidence they have to date. If they have enough information and probable cause to believe that there is a crime about to occur, or a crime has occurred and they need to find out information, they will get a warrant for interception of communications. If they do not have enough information to convince a judge of that higher burden, they will apply for access to the communications data.

Lord Faulks: So it is bespoke.

Dr Hosein: Yes.

Nick Pickles: But on the GPS warrant case specifically, it was argued on the point that putting a GPS tracker on someone’s car constituted an illegal search of the individual. It is a slightly different nuance there, but they came to the conclusion that just tracking someone’s location constituted a personal search, and therefore should be warranted.

Q121 Baroness Cohen of Pimlico: There is a temptation to think, and I thought the Home Office was almost saying to us, that you kind of get a huge sweep of information without being that intrusive.

Nick Pickles: Would that be the filtering proposals they were discussing?

Baroness Cohen of Pimlico: Yes, if you just go for whether a communication has taken place, you get a huge sweep of information, very useful to you in pinning down your investigation, and not that intrusive on the citizen.

Jim Killock: What is intrusive is all about context, is it not? If I am e-mailing Alcoholics Anonymous on a regular basis, that is pretty indicative of what I am talking to them about. Similarly, if I am communicating with a group of individuals on a particular issue through a particular website, or something, that tells a lot about my political opinions and my political organisation, and perhaps even my decision to protest at a particular point. Similarly, if a journalist is communicated to by somebody who is on a list of potential leaks, the mere fact of communication pretty much tells you that they are the person you might want to arrest. Traffic data is actually incredibly intrusive, and that is why it is useful, but that is also why it needs to be regulated very tightly.

Mr Davis: I mentioned earlier Malte Spitz. I was talking about telephones rather than e-mails there. When the German court struck down the German law that is the RIPA equivalent, not this equivalent, he obtained from Deutsche Telekom six months’ data on his own telephone.
He thought he would get a few hundred telephone calls. What he was given was 35,000 data points of where he was for every five minutes of his waking life. It is on the web, if you want to look—you can search under Malte Spitz. Basically that man had a tracker on him. This is intrusive in all sorts of ways. I could give you half a dozen other examples, but that may give you a measure.

**Baroness Cohen of Pimlico:** Yes, I agree.

**The Chairman:** Mr Brown, I am conscious that we are on a very tight schedule.

**Q122 Mr Brown:** We are rapidly moving up against the bell. Two points: firstly, have you anything to say to us about the danger, if you advocate a warrant system rather than a senior official authorising a junior one, of tame magistrates, in other words of people choosing which magistrate they will go to because of their known position on these matters? Secondly, it has been put to us that the reason why public officials dealing with sensitive data do not send it to newspapers or sell it on to people who can make commercial use of it is that they would be caught and punished. Are people caught and punished? Is there anything you could say to us on that as a sanction? Does it work?

**Mr Davis:** In your previous life you must have come across cases where data about Members of Parliament was sold by policemen time and again.

**Mr Brown:** This is the point I am getting at.

**Mr Davis:** Yes.

**Mr Brown:** They do not seem to be caught; they do not seem to be punished; and in the case of the offence of misconduct in public office, there is a ruling by a judge that says it was not committed seriously enough.

**Mr Davis:** What is the point you are driving with this?

**Q123 Mr Brown:** Is there anything you want to say to us about the effectiveness of that as a sanction?

**Mr Davis:** I think it is an effective sanction. It would be quite interesting for you to question the officers who searched Damian Green’s office as to what happened when they tried to get a warrant. I think you would find that would be quite interesting. The simple truth is that you have to manage the warrant process as you would manage anything else, and not allow the same magistrate or the same judge to be asked every time, and set certain levels of evidence required for the magistrate. It is not simply a handover to somebody else; it is actually a structured process.

**Nick Pickles:** On the penalties point, I would simply say that I hope the Information Commissioner has been at the heart of the Home Office’s discussion about this Bill, because he is responsible for an awful lot of regulation. Right now the Information Commissioner cannot walk into my local GP surgery without their permission, let alone Vodafone or a commercial services provider. If he does find wrongdoing, breaching Section 55 of the Data Protection Act does not carry a custodial sentence.

**Mr Davis:** It should.

**Nick Pickles:** I think we have had a clear call from the Justice Committee to say this should happen. I think the Leveson inquiry would have been avoided had that been available and been prosecuted, and that is on the statute book; it just has not been enacted.
Q124 Lord Strasburger: Dr Hosein, in your opening remarks you threw away a rather stark statement, which was that these sorts of measures have not been taken up in any other democracy. Would you care to elaborate on that?

Dr Hosein: The collection of data through black boxes at ISPs in order to monitor activities within a country and beyond a country has only been implemented at a national scale in China, Iran and Kazakhstan. DPI—deep packet inspection—and black boxes have been used on a local scale, and we have cases in Egypt, Pakistan and Tunisia. The idea of a black box run at a national scale, at an organised centralised level, as to what will actually be monitored, has not yet been done in a democratic country.

Q125 Lord Faulks: I would like to ask you about permitted purposes. The Bill lists quite a number of permitted purposes for which communications data can be obtained. I think they are based on RIPA, although there is also a power under which the Secretary of State may order an addition to the permitted purposes already listed. Are you concerned about the range of permitted purposes and, if so, which particular categories concern you?

Mr Davis: It would be quicker to say what is not permitted.

Nick Pickles: Yes.

Mr Davis: I am concerned about preventing disorder, given what we had with the police handling of a number of environmental protestors on that front. Financial services are restricted: fine. As for economic well-being in the United Kingdom, interest of public safety, over and above detecting crime and terrorism, public health—are these serious things? What we have created here is the longest possible shopping list the Home Office could come up with. You could probably get away with national security, preventing and detecting crime, the financial services stuff, investigation into alleged miscarriages of justice, and a final category of a dead or disabled person. The rest, I think, are otiose.

Nick Pickles: I apologise, I forget which Member of the Committee yesterday asked for the scenario—Lord Chairman, it may have been you—as to what situation could arise where a single request could affect multiple individuals. Indeed, a reading of preventing disorder may be that, in the case of a protest outside Parliament, you would want to know the identity of every mobile phone within a half-mile of Parliament Square. There will be a way of identifying people who will be on a protest. It is a natural extension of what the Metropolitan Police currently do with their forward intelligence teams, who hold photographs of individuals, which has just been ruled unlawful. The scope for this is not just the types of offences, but also the manifestations of the new technology, which could then be applied, as Mr Davis says, to what is an incredibly broad list, which should be cut down under the existing law.

Q126 Lord Faulks: I suppose you could think of individual cases that might not easily fit into limited categories, hence the expansion where, given the particular facts, you would say it was reasonable to obtain that information. Presumably that is the purpose.

Mr Davis: Frankly, Lord Faulks, I would challenge anybody to answer: if it is not in the interests of national security, it is not for preventing or detecting crime, it is not under the very specifics of the FSA, or where somebody is injured, or the miscarriages of justice, why is it in the category? Give me an example which fits. There are cases that will be about protecting public health, but they will be a crime, almost certainly, and ditto public safety. It is very hard
to think of a real example, and this would create a complete open sesame here. It is not good law.

Nick Pickles: This is for the obtaining of communications data, not the disclosure of communications data, so I think that is an important distinction to make.

Dr Hosein: Traditionally we have had limitations placed on some investigations. We have said you cannot breach privilege, for instance. RIPA erased all those previous limitations on the cases and types of situations where you get access to information. In some countries they limit the purpose of an investigation. If it is linked to, as the example was used, political protest, the practice of free expression, or anything having to do with your religion, then you cannot conduct that investigation at all, unless another crime is being conducted. It would be nice to see those types of limitations.

The Chairman: Dr Huppert, you might get a couple of words in.

Dr Huppert: Thank you. Very quickly, we have been assuming throughout all this—the Home Office were assuming yesterday—that there was a very clear distinction between communications data and content. How sure are you that those are completely separate? Would the proposals in the Bill perhaps lead to content being collected, and in particular could any black boxes collected—

The Chairman: I will need to stop you there because of the Division. Ladies and gentlemen, in a moment I will adjourn the Committee. This is the start of a series of Divisions in the House. This has been an exceptionally good evidence session; I regret that we have to conclude now and will not be able to hear from you again today. We have a series of questions we would have liked to ask you. We will submit them to you, if we may. You may be sending written evidence in any case; if you could address these questions we would be grateful. Thank you very much for attending. I adjourn the Committee until our session tomorrow.
THURSDAY 12 JULY 2012

Members present:

Lord Blencathra (Chairman)
Lord Armstrong of Ilminster
Lord Faulks
Lord Jones
Lord Strasburger
Mr Nicholas Brown
Michael Ellis
Dr Julian Huppert
Stephen Mosley
Craig Whittaker

HMRC [Donald Toon], Metropolitan Police Service [Cressida Dick], ACPO [Gary Beautridge], SOCA [Trevor Pearce] and CEOP [Peter Davies] (QQ 127-185)

Examination of Witnesses

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

Q127 The Chairman: Welcome to the third public evidence session on the Communications Data Bill, and welcome to our panel of witnesses. We are under a tight time constraint. We have a lot of witnesses to hear from today, a lot of evidence we wish to gather and a lot of questions we wish to ask. Perhaps we could crack on by asking the members of the panel briefly to identify themselves and then we will start with the questions.

Peter Davies: My name is Peter Davies and I am Chief Executive of the Child Exploitation and Online Protection centre.

Trevor Pearce: I am Trevor Pearce, Director General, Serious Organised Crime Agency.

Donald Toon: I am Donald Toon, Director of Criminal Investigation, HM Revenue and Customs.

Cressida Dick: I am Cressida Dick, Assistant Commissioner in the Metropolitan Police.

Gary Beautridge: I am Gary Beautridge, Assistant Chief Constable, Head of Kent and Essex Serious Crime Directorate, and I chair the Data Communications Group for ACPO.

The Chairman: We have a lot of questions that you might all want to answer, but if every one of you responds to every single question we will be here until midnight. All of you do not have to answer each question. Feel free to select from among yourselves who is going to take the lead, but do not be constrained; if you have something to say, say it.

Q128 Dr Huppert: Can I start off by understanding how things operate under the existing laws? Can each of you say briefly how much communications data you currently use; how many requests you made in the last year, and to how many people did that apply; what were the purposes; and how many cases were successfully prosecuted or concluded?
Peter Davies: I cannot give you all that data. I am happy to supply it in writing later on. As a general overview, we make roughly 3,500 applications per year. A proportion of those are unsuccessful. We are slightly unlike some of my colleagues represented here, in that we do not then make arrests, for example. We pass high-quality intelligence on to others, including law enforcement and community and children’s services, so they can make safeguarding interventions or arrests. That is a picture of the volume. Something that slightly distinguishes us is that the vast majority of those are communications related to online activity, so ours is a slightly different picture.

Trevor Pearce: Our focus is on serious organised crime. About 95% of my investigations will have some kind of communications data attached to them. For example, in April and May, of 13 cases prosecuted by the Crown Prosecution Service on our behalf, 12 had communications data fundamentally at the centre of them. In relation to the specific numbers, we are happy to follow up in communication.

Donald Toon: In 2011, we had 5,000 applications and 15,270 individual items of data. To give an indication of the impact, that is directly related to about £850 million of protected revenue in a significant number of cases.

Q129 Dr Huppert: In one year.

Donald Toon: In one year.

Cressida Dick: The Metropolitan Police have responsibility for a large proportion of serious crime, organised crime, counterterrorism and other forms of crime, so we use this in preventing and detecting crime. We also use it hugely in terms of saving people’s lives where there is an imminent threat to their lives. If I take the example of terrorism, we are the agency that, with the Crown Prosecution Service, brings evidence to court, so we present this data in evidential form as well. I cannot give you the exact figures, but we are by far the biggest police service and have much the biggest use of communications data.

Q130 Dr Huppert: But you would be able to send us the figures on the people, cases and requests.

Cressida Dick: I will certainly attempt to send you the figures you are looking for.

Gary Beautridge: In my two force areas, last year there were 10,107 applications, of which at the point of first contact 2,577—25.49%—were declined as not meeting the standard by our single point of contact. A further 112 were later declined by the dedicated person who reviewed these incidents. We have recently conducted a national two-week survey in respect of the number of applications, and I can provide that in written form to the Committee, should that be required.

Q131 Dr Huppert: I look forward to seeing more of that data. You clearly make considerable use of communications data at the moment, although I am slightly concerned about the 25% that are declined. What is not clear is the data that currently you cannot get. The Home Secretary has spoken about Facebook and Google. As I understand it, Facebook and Google do comply with a number of requests. What is it that you cannot get from them at the moment?

Cressida Dick: I am not technically qualified to tell you that. What I can say is that when I sit down with my senior investigating officers, both in counterterrorism and serious crime, they
say they all have experience of not being able to get the data they would like, and they are feeling that increasingly.

**Q132 Dr Huppert:** But you do not know what sort of data it is. If Google said they would provide you with anything you asked for, you could not tell them what you wanted.

**Cressida Dick:** I am never myself an applicant. When we apply we are always very specific as to what we are looking for. There is an increasing amount that is either impossible or difficult to get.

**Q133 Dr Huppert:** Can you tell us what it is that is missing? We are trying to understand what gap needs to be closed so we can work out how to close it.

**Cressida Dick:** It would be difficult, for reasons you would understand, to be hugely specific about the precise type of data, or indeed the companies in some cases, because that is something that we, sitting here, do not want to tell all the criminals right now.

**Q134 Lord Armstrong of Ilminster:** Is it because the information is not available or because it is withheld by the service providers?

**Cressida Dick:** My understanding is that it is more often not available, and increasingly so. Occasionally, it is also withheld.

**Q135 Dr Huppert:** I think that both Mr Beautridge and Mr Davies want to comment.

**Gary Beautridge:** In some regards we do not know what we do not know. There is, however, a lot of information being requested through our own single points of contact that we know is not available. To open that up publicly would expose some vulnerabilities within the service. We would very much like to take the opportunity to write in on that specific point, which would illustrate the type of information we do not have access to.

**Q136 Dr Huppert:** I think that would be very helpful.

**Peter Davies:** I would like to echo that. There are two points. One is that there are certain types of data not currently available through any legislation that are gaps that we do not want to expose to the public, for reasons Commander Dick has highlighted. The other is that some providers are better, quicker and more comprehensive in providing the data on request than others, so some of this is occasionally about which provider you are going to ask and you have a different level of confidence in the likelihood of a reply.

**Q137 Dr Huppert:** Presumably, none of you has seen the draft order that would go with Clause 1 of the Bill. Do you have any way of knowing whether the data you are currently lacking would be acquired even under this legislation?

**Cressida Dick:** Speaking for myself, I believe this is absolutely fundamental. I would like to maintain our current capability. I am not technically qualified to describe how we would do that.

**Q138 Dr Huppert:** If there are people in your organisations who have the technical information that would be helpful to this Committee, we would appreciate seeing it.
Trevor Pearce: It may assist this Committee, as we have done with others, certainly in relation to SOCA because of its wider responsibilities around broader technical issues, if we offered the opportunity to come and take a briefing and watch this in action so we can provide more context to the answers that we are not able to give here.

Cressida Dick: We would all very much like that.

Q139 Dr Huppert: That might well be helpful. A number of the communication service providers overseas, which I understand from what the Home Office and Home Secretary have said are part of the issue, are based in the US. There are a number of other countries. There are mutual legal assistance treaties between us and the US, so presumably it would be possible to get data from them direct from source using the MLAT approach. Have any of you used that or had experience of doing that? You must do that in SOCA.

Trevor Pearce: It can be used through letters of request, but it is about the nature of what you can ask for. In some regards perhaps a specific piece of information can be obtained. More broadly, in terms of how you carry out an investigation when you are seeking a range of conspiratorial material, that is a greater challenge.

Peter Davies: I would agree with that. Where we go abroad, there are also issues in terms of duration of data retention, particularly in the online world. There may be some delay between the piece of data being sought and the request being submitted. There are MLATs and international letters of request, but there is a delay involved and that is where the time limit comes in. Some of the attrition in getting data back is due to the expiry of the time limits.

Q140 Dr Huppert: How long a delay? Does that just argue that the MLAT process could be made faster?

Peter Davies: I do not think it is necessarily all about that. I cannot give you an exact figure for the delay. What I can tell you is that if, say, we worked on the principle of retention for 12 months, there are some aspect of our investigations for which that would still not be long enough, and there is a delay in doing the international best process.

Gary Beautridge: There is certainly an inconsistency of approach among different CSPs that are not located within this country. We approach them for information and evidence. Some supply it in the format required; others do not. At the moment, there is not a consistent approach to the provision of this information by overseas providers. I could also provide specific examples of that, should that be required.

Q141 Craig Whittaker: In what proportion of your overseas requests do you get no information at all? Is that a big problem for your organisations?

Cressida Dick: I would have to research that. With the Chairman’s permission, we would intend to give a written submission later, and we can put that into it.

Peter Davies: That would also be my response.

Q142 Stephen Mosley: We had quite a disruptive session yesterday because of the sceptics. A couple of them said, “We’re all carrying round in our pocket a tracking device”—one of these—and one of their concerns was the availability of passive information between a mobile phone and mobile base station. Would you want that sort of communications data within this Bill?
**Peter Davies:** For some time it has been possible, roughly or more precisely, to locate a mobile telephone through the use of communications data. A team I have led has used that as almost the sole means of detecting a serious double murder in one of my previous forces. I do not think that is a novelty. I do not quite understand the distinction between a smart phone, to which you are referring, and what has already been available for many years, which has helped protect the public and prosecute offenders in the past with less developed technology and mobile phones.

**Stephen Mosley:** Essentially, that communication would be classed as communications data as far as concern the law enforcement agencies.

**Donald Toon:** In terms of the identification of a location, certainly it would be classed as communications data.

**Q143 Lord Strasburger:** To seek clarification on MLAT, presumably that is two-way and gives the Americans the opportunity to make inquiries of whatever data we are retaining. Is that the case?

**Peter Davies:** The legal assistance process allows third-party states to make requests, if those requests are able to be made within the UK.

**Lord Strasburger:** If, as a consequence of this legislation, we expand the amount of data we are retaining, the Americans would potentially have access to that through MLAT.

**Trevor Pearce:** If the right consideration is in place.

**Peter Davies:** Anybody with whom we have a mutual assistance treaty would technically have access, but of course that would go through some kind of decision-making process in the UK.

**Q144 The Chairman:** ACC Beauchridge, you were able to give us detailed figures for your own force area, Kent. Would it be your understanding that every police force in the country would have exactly the same sort of data in the same detail?

**Gary Beauchridge:** They should have that type of information, and it should be capable of aggregation and submission to this Committee.

**The Chairman:** Do you submit it routinely to the Home Office?

**Gary Beauchridge:** It is submitted routinely to the Information Commissioner.

**The Chairman:** But to the Home Office.

**Gary Beauchridge:** In the annual inspection.

**The Chairman:** The Home Office should already have the aggregated figures for all the police forces in England and Wales.

**Gary Beauchridge:** I believe that should be the case.

**The Chairman:** That is very helpful.

**Q145 Michael Ellis:** The Government have emphasised the importance of communications data, particularly as regards law enforcement, security, intelligence agencies and the like, in apprehending criminals and protecting the public. Could each of you briefly say something about how important you perceive this data acquisition to be in your individual experiences? For example, Mr Toon, I think you said a few moments ago that as far as the Revenue is concerned, it was able to secure £850 million last year.

**Donald Toon:** That is correct. There is a range of data we obtain through communications data authorisations. 80% of what we obtain is section C data; essentially, it is a straightforward
subscriber check. It enables us to identify individuals who are involved in a fraud and further the investigation. If you want specific examples, we had an operation that led to the conviction of Mr Kevin Burrage for alcohol excise diversion fraud.

Michael Ellis: How much was that worth?

Donald Toon: That particular fraud was £50 million a year. He was sentenced to 10 years in prison as the major perpetrator. He had been operating for a number of years, seeking to undermine the alcohol duty control system.

Michael Ellis: So, it is worth nearly £1 billion a year to the Revenue.

Donald Toon: Yes. One interesting point to go along with that is that the £850 million refers to the direct revenue loss prevented as a result of the investigations we carry out. In addition, often we use the results of the investigation to change our internal processes and procedures, or on occasion to advise Treasury and Ministers about potential changes to the law. That protects a significantly greater proportion of revenue.

Q146 Michael Ellis: Mr Davies, could you say something about how it has assisted child protection?

Peter Davies: You asked for personal experience. Can I offer just one example prior to child protection? The double murder inquiry I mentioned related to a retired couple shot dead in their home on the coast of Lincolnshire in August 2004 by, as it turned out, the pre-eminent organised crime group then operating in Nottinghamshire. Bluntly, without communications data relating to contacts between mobile phones it would not have been possible to detect that crime and lock up the people responsible. For all I know, they might still be operating in Nottinghamshire now had that not been possible.

Q147 Michael Ellis: That is one double murder in your experience.

Peter Davies: That is a double murder, but I think it illustrates how long this goes back in terms of being an issue. Bluntly, there were other people involved in the conspiracy whom it might have been possible to prosecute and convict, but who it was not possible to prosecute and convict because there was a data loss in that investigation.

To give a more recent example, a force for which I was responsible in operational terms commenced an inquiry into a small group of people operating a news group, facilitating the circulation of child abuse imagery on a worldwide basis with over 2,000 members. The force I was involved in led the investigation. In the course of that investigation, 132 children in the UK were safeguarded and protected, and nearly 200 suspects were arrested and a large number brought to justice. The four people at the heart of this news group operation, which was run for profit and, regrettably, enthusiasm, were convicted. Again, without access to communications data, those outcomes would not have been possible. With access to fully retained and accessible communications data, more people might have been brought to justice and more children safeguarded.

Michael Ellis: To be clear, you are saying that 132 children were safeguarded as a result of your access to communications data.

Peter Davies: Yes.

Michael Ellis: But you feel that, because of current gaps in your powers, some have not been safeguarded.

Peter Davies: Absolutely.
Q148 Michael Ellis: And some child sex offenders and paedophiles are getting away with it. Peter Davies: Yes, and that is still the case today from my current perspective in CEOP. A third example: one of the things we do on a daily basis is help ChildLine in identifying children who contact them over the internet rather than by telephone. Frankly, it is inconceivable to me to envisage a society where law enforcement, or people like ChildLine, are denied the opportunity to identify children at risk of suicide, locate them and get the right thing done about them. That is more or less a daily occurrence in CEOP at the moment. We experience data loss there and with some of the serious offenders we are dealing with. There are more examples, but I need to be brief.

Trevor Pearce: If I may focus on two areas, in 240 cases last year we were able to prevent either threats to life or kidnaps; that is, attacks which would have taken place against members of the public. If those had taken place, we know that the cost of an average investigation into a murder is about £1.8 million, so, notwithstanding the issue of family and personal injury, there is a fiscal cost to this as well.

Secondly, 95% of our investigation will have some kind of communications data in place. Communications is one of the key enablers for organised criminals to operate. The range of communication capabilities they now have enables them to operate more conveniently for their purpose, and therefore that has to be available to us if we are to show the true extent of conspiracies. A significant number of our investigations go into the criminal justice system, and the process by which that communications data was acquired can be tested in court procedures, as well as the evidential interpretation of the material that is gathered.

Q149 Michael Ellis: As far as this point is concerned, you say there were 240 serious organised criminals—people involved in kidnapping and other very serious offences—in the last 12 months.

Trevor Pearce: No. Those were 240 potential threats to life averted through access to communications data, whether that is kidnapping or a significant contract to kill.

Michael Ellis: You put a cost of approaching £2 million on each investigation if you had not had the data.

Trevor Pearce: That would be right.

Michael Ellis: That is approximately £500 million saved by having the data.

Trevor Pearce: Yes.

Michael Ellis: Have you been restricted or obstructed because you are not able to access communications data at the moment in other investigations?

Trevor Pearce: As in previous answers, there are opportunities lost or not available, and we are happy to go into those in more detail.

Q150 Michael Ellis: Assistant Commissioner Dick, how do you feel about it from the perspective of the Metropolitan Police?

Cressida Dick: At the risk of echoing some of what my colleagues have said, from the point of view of the Metropolitan Police, if I take, as I did the other day, a completely random week, we would expect to have one kidnap, which is the sort of operation in which we are putting an enormous amount of resource, where communications data is absolutely fundamental. About five suicidal people will be found through communications data. We probably have an
abduction—perhaps an honour-related abduction, or something like that—and other threats to life.

As to murders, speaking to my senior investigating officers, it is now extraordinarily rare to have a murder in London where communications data is not a fundamental part of the investigation. Indeed, if we look at Trident gun crime murders, which colleagues will probably be familiar with, in every single one communications data is fundamental to the investigation. You have very few witnesses; usually you have limited forensics; you are very limited in what you can do, but often there is a call from the offender to the suspect, or through another person, before the time. It is usually a group of people. They get together and communicate before and after. It is a vital part of our investigation.

As to robberies and rapes, it is very usual for phones to be stolen. The stranger rapist, on many occasions, will take the phone from the victim and within 24 hours we find the rapist.

If I turn to counterterrorism, you will be aware that every single major security service and police counterterrorism operation involves communications data. Looking at those that are very obviously in the public domain, in the 7/7 investigation communications data was very obviously extremely important. If you look at Seagram, which was the Glasgow attacks, we tracked them to Glasgow and found the bomb factory. For all of them we use communications data all the time, and the important thing is that the police use evidential communications data in these investigations.

**Q151 Michael Ellis:** This Bill seeks to redress a mischief. Both the Home Secretary and the Justice Secretary have indicated that there has been a degradation, which has been approximated at 25%, of the data that can be obtained by police and security services, so we are down to 75% of data. Are any of you able to share with us—those of you who have not already done so—any instance where this inability has impacted on the conduct of your investigation or prosecution of a case? Are there examples you can give of people who have not been prosecuted, despite the fact your investigating officers knew or believed they were involved in a ring or some other organised crime, because the evidence could not obtained?

**Gary Beatridge:** I could certainly point to cases where there have been prosecutions in spite of not having earlier access to that data and we have only found out the activities of the individual in question significantly after the events have occurred. The most recent case under my command was the rape of an eight-year-old boy and 10-year-old girl. We could not get the information we wanted and had to employ other techniques, which were ethically and technically extremely complex, expensive and lengthy, to bring the offender to justice because of the method of communication the offender was using, which was web-based communication. We have other cases, most recently one where three people were convicted of a triple murder, and the speed of the investigation was very much directed as a result of access to more conventional communications data. We could get on top of the case immediately and save hundreds, if not thousands, of man hours. We tracked the offenders from Coventry to Chatham in Kent where they set fire to a house and murdered three people. That is the opposite side of the spectrum to show how digital footprints are now key; they are not a “nice to have” but intrinsic to investigation and the core function of policing, which is looking after vulnerable people. That allows us to do that.
Q152 **Michael Ellis:** What are the categories of additional data that you would wish to be collected that providers either do not currently hold or you are not currently allowed to have access to under the legislation in situ that you believe would be necessary for investigatory purposes?

**Gary Beautridge:** I think that would expose publicly some of the vulnerabilities of law enforcement. With your good grace, we would prefer to be able to submit written evidence in that regard.

**Michael Ellis:** Speaking for myself, I do not press you on that. As far as concerns this Bill, however, you are familiar with the terms of its clauses. Do you believe this Bill would redress some of the current gaps in policing as far as concern these issues?

**Gary Beautridge:** I do, absolutely, yes.

Q153 **The Chairman:** Some of the critics of the Bill have said that often you are looking for a needle in a haystack, and if we now give you an extra few billion bits of evidence we have just made the haystack bigger. What is your response to that?

**Gary Beautridge:** I would not agree with that position. Whatever we do, there is a proper intelligence and evidence base for making the application. Applications are made on the basis of necessity and proportionality. What should not be forgotten is that there is a real financial cost in getting this information, and a further cost if it needs to be presented evidentially. These matters are very carefully considered. The applications are made on the basis of intelligence, evidence and in furtherance of criminal investigations.

**Peter Davies:** The issue is partly to do with the assumptions that lie in the question. One of the key assumptions is that it is possible to make entirely speculative communications data requests and get them authorised. My experience is that that is simply not the case. More typically, one is confronted with a situation where, often after the fact, one wants to reconstruct a criminal network from one or two people.

Q154 **The Chairman:** You have a suspect in mind.

**Peter Davies:** Organised crime works through networks, and one has to reconstruct the whole network. The risk is that, if you settle for one part of the network and lock up only that person, the rest of the network is free to carry on offending. The concept that this is purely speculative is against all my experience and the procedures that currently apply.

**Cressida Dick:** If it is possible, I urge you to come and see one of our units, look at the application forms and talk to our staff. It is extremely precise and incredibly well supervised and scrutinised. It is not looking for a needle in a haystack on any occasion.

**The Chairman:** The Committee will consider seeing, either at SOCA or somewhere, how the data is inputted. We will probably want to study that in situ somewhere.

Q155 **Lord Strasburger:** Can we turn to the current authorisation arrangements under RIPA? The draft Bill has been criticised for not requiring public authorities, other than local authorities, to seek any independent authorisation to obtain communications data. Instead, a senior designated officer in the same organisation must authorise any request. How does this system presently operate in your organisations?

**Trevor Pearce:** The application is made to the SPOC who will advise before going on to the designated person, who can give authorisation, and then the CSPs. The notion is that, as well
as making judgments about the legality and process around proportionality, necessity, etc, you need a degree of operational understanding, not in relation to the operation or activity taking place, where quite rightly there must be some degree of separation, but about the practicality of that as it fits in with an investigation or inquiry, and, certainly from the perspective of my organisation, the nature of the investigation.

**Donald Toon:** From my perspective, it depends. There are two levels of authorisation. In relation to the lower category of data, section C subscriber check data, we have 100 officers specifically trained to act as designated persons in relation to that data. The application goes from a case officer through a more senior verifying officer before it goes to the designated person for a decision, and then on to the CSP. I have three people in one specialist unit who are designated persons for all applications for the 20% of our requests that are for higher-level, more sensitive data.

**Cressida Dick:** It is very similar for us. We have two levels—the inspectors and superintendents—as the designated persons. The vast majority of our requests are in relation to subscriber checks. The officer goes through a supervisor. They seek advice from the single point of contact, who is a very highly trained person. They then put in their application. It goes to the designated person who comes back through the single point of contact. The designated person in the Met is almost never even in the same unit as the person who is making the application, and the people who are operating as the single point of contact are in a specific unit. They work together all the time, and they are also completely independent of the applicant.

**Gary Beautridge:** From my perspective, there are very high levels of professionalism around this similar to Assistant Commissioner Dick’s summary. Last year there were 10,107 applications in Kent and Essex. These are made primarily either by detective constables or detective sergeants who are officers in the case. The applications go to a separate unit entirely divided from those officers and are assessed at the single point of contact. At that single point of contact, 2,577 were rejected. When they subsequently went through to the designated person, who is a superintendent—a very senior officer—a further 112 were rejected. Everything is looked at on the basis of necessity and proportionality. If it is for the investigation of crime and protection of vulnerable witnesses or people, we need to make sure that all the human rights considerations are properly considered and there is a process of justification that sits behind it. We would not want well-meaning individuals wading through a thicket of confusion around these issues. These are highly trained specialists who do this all the time and make proper decisions on the applications.

**Peter Davies:** I would like to make a more general point in answer to your question. I think I speak for all my colleagues, here and not here, in saying that we absolutely understand and respect the requirement to balance the occasional need for intrusion with a proper, transparent and accountable process to make sure the innocent are properly protected. In one or two of the conversations I have had on this issue previously I have sensed people have assumed that people would be better protected if there was an alternative means of providing authorisation. Can I invite you to take a very objective view about the realistic possibility of those alternatives, the cost of those alternatives and whether they are more likely to protect the innocent than the safeguards my colleagues have described? I echo that it is really important, if it is at all possible for you, to go and see the process in action, because I think it brings it to life.
Q156  **Lord Strasburger:** Can you tell us how many convictions or disciplinary proceedings there have been for misuse of this system?

**Trevor Pearce:** In my organisation, none.

**Donald Toon:** We have had none in our organisation. Interestingly, we have issues about other forms of sensitive data, for example taxpayer data, where we dismiss staff regularly for breaches there, but I think the zero figure for us reflects the fact that this is a very closely controlled area with authorisation requirements before there is any access to the data itself.

**Gary Beautridge:** If we want the public to have confidence in the use of data like this by the police we have to take its guardianship very seriously, as we do. In respect of data breaches, the sanctions are extremely severe in Kent and Essex. We had one recent case, which I cannot talk about in detail because it is still going through the judicial process, where something linked to this type of issue has resulted in a criminal charge against a member of my organisation. That is currently going through the process.

Q157  **The Chairman:** ACC Beautridge, do I understand correctly that you are saying to the Committee that the civil liberties of the individuals and their privacy is better protected by a trained superintendent in the police force than by well-meaning individuals who may be magistrates?

**Gary Beautridge:** That is absolutely not what I said. I said that within the police service we do not want well-meaning amateurs dealing with these applications, which is why we train officers and designated persons to a very high level. Nationally, over the last two years, over 10,000 people have been trained in the use of communications data. That was absolutely not what I meant. I meant that we do not want an artisan approach within the service to deal with this very complex area of business.

Q158  **The Chairman:** I am glad of that clarification. I thought it was a general description of the magistracy. I want to be very careful here; I do not want to ask about a criminal case. In principle, would you be averse to having a criminal penalty in this Bill for officers of any organisation who break the rules?

**Gary Beautridge:** I cannot answer on behalf of ACPO in totality, because I have not discussed it with my colleagues. As a personal view, I would not be against that. This is a very serious issue.

**Trevor Pearce:** We are certainly used to it in other parts of the Regulation of Investigatory Powers Act, notably Part 1, so attaching criminality to communicating certain procedures or processes in place is already in the current legislation. We recognise it as absolutely vital in protecting those equities.

**Cressida Dick:** I can speak for the Commissioner and say we take any breach of any data incredibly seriously. We have had examples, not specifically to do with communications data but more generally, of data protection breaches and others, which we will pursue as far as we possibly can. Regularly, sadly, people end up in court for misconduct in public office, occasionally for computer misuse and data protection. Those are very powerful bits of legislation. If there was to be another aspect to this Bill, how on earth could we object to that? But we do already take this very seriously.
Q159 The Chairman: I appreciate there is a range of criminal sanctions in other legislation that could catch people here. I know that Parliament is always in danger of adding a similar criminal penalty to every bit of legislation when it is already there. Do you think it would reassure the public if there was a specific criminal charge in this Bill?
Trevor Pearce: Yes.
Cressida Dick: I can see that.
Peter Davies: I have probably the dubious distinction of having personal experience of the consequences of these things not being done properly, not, I have to say, on my own part. In a force I worked in previously, processes were put in place that were below the standard expected by the Regulation of Investigatory Powers Act. The consequences were, first, that three expensive serious crime inquiries failed at the prosecution stage. The consequences for the officers involved, whether or not they were closely responsible for these problems or just associated with the inquiry, were very significant in terms of lengthy external misconduct inquiries and, for those responsible, sanctions. One of the other drivers for quality in this is the knowledge that a prosecution might fail because of lack of proper process being applied.

Q160 Michael Ellis: Each of you spoke of your own public authorities and how infrequent prosecutions or disciplinary action had tended to be for offences of this sort. Assistant Commissioner Dick, have you far more experience of dealing with misconduct in a public office for misuse of the police national computer, for example?
Cressida Dick: I regret to say that we do. Data misuse is a considerable risk for all police forces given the amount of personal data we have. Other systems are more vulnerable and easier to get access to than communications data.
Michael Ellis: Under the current legislation.
Cressida Dick: Yes.
Michael Ellis: You would say that the absence of prosecutions for communications data breaches, when juxtaposed with prosecutions for misuse of the police national computer, for example, is a reflection of the current security within the system as far as concerns communications data.
Cressida Dick: Absolutely. There is a very strong security regime around communications data.
Michael Ellis: Much stronger than for the police national computer, for example.
Cressida Dick: The nature of the police national computer is such that every single officer and some police staff, with some safeguards, can have access to it. The databases on which we keep this information are not the same at all.

Q161 Lord Faulks: I suppose that access to the police national computer gives you an idea of how these things can be misused. I appreciate what you have all said about the safeguards in existence. Do you think that such risk that it is, which you are protecting against, is a collateral use of material, or simply over-enthusiastic investigation?
Cressida Dick: When I was answering the last question, I was talking about deliberate leaking of information, potentially for money. The dangers of collateral intrusion are in the minds of all designated officers, and everybody who works with RIPA in all its aspects, all the time. We have to look constantly at the risk of collateral intrusion and how we will reduce and mitigate
it. If there is a significant risk of collateral intrusion, which we regard as disproportionate and inappropriate, we will not authorise anything.

**Q162 Lord Strasburger:** There were 552,000 applications for data in the last year for which we have figures. I know that you collectively do not account for all of those but you probably account for a good number of them. I think that collectively you revealed to us one case of malpractice in applying for this data, if I am correct. There are probably only two possible explanations for that. The first is that your systems are incredibly watertight, and the other one is that you are not aware and not detecting misuse when it is happening. Do you accept that?

**Gary Beattidge:** I referred to one case within Kent and Essex. We could research if there have been other cases across the country. I think that to make the presumption on the effect of the one case in Kent and Essex and apply it to the national figures would be a dangerous thing to do. That would require more research.

**Q163 Craig Whittaker:** On the 552,000 applications, what proportion of those would you say are used in serious crime? We heard yesterday about applications also being used to chase up speeding fines, for example.

**Gary Beattidge:** I can answer some questions based on the recent national survey we have done over a two-week period. The results of that survey indicate that 72% of the data requests related to suspect inquiries, 18% to victims of crime, 2% to witnesses, and 8% to other issues, such as missing persons and vulnerable individuals. The results of that two-week survey could be made available to the Committee, should you require it.

Part of the remit of my day job is to tackle serious organised and economic crime within Kent and Essex. The recent national mapping of organised crime groups indicated there are over 8,000 nationally, and over 30,000 members of those groups. From my own experience over many years, an armed robber does not commit just armed robbery. People who are in this for financial gain take a blended approach to criminality for financial gain. If a burglary could release sufficient funds to somebody who commits armed robbery, they would commit that as well. When we are tackling organised crime groups, we will take them out in whatever way we can, as long as it is lawful and ethical. It is not just for the more substantive serious crimes; if we can take them out by other means, that is what we do. The use of communications data is intrinsic and absolutely vital to those investigations.

**Q164 Craig Whittaker:** I understand that, but my specific question was: what proportion of the information requests are for those serious crimes compared with non-serious crimes?

**Gary Beattidge:** We could certainly look to disaggregate that from the recent survey conducted over a two-week period nationally and supply that to the Committee.

**Cressida Dick:** For the Metropolitan Police, I can say that a large proportion is for serious crime. Obviously, there are different definitions of serious crime, but, however it is defined, they are what anybody would regard as serious crimes. You may have heard the commissioner quote the figure of 23%, or roughly a quarter of our requests, over the last five years being for murder. Within our murder and most serious crime investigations—I am sure colleagues to my right would say this as well—we tend often to make multiple requests. In counterterrorism
we will make multiple requests for one particular case, so the less serious the smaller volume of requests in the case.

**Q165 Craig Whittaker**: What would be the impact on your organisations of a system that required you to seek prior judicial authorisation of all requests to access data?  
**Trevor Pearce**: We would need to leave in place our internal processes, because that gives us the quality assurance and operational oversight that we require. There will be security, cost and bureaucratic considerations. The more significant consideration, particularly around some of our responsibilities in relation to threats to life, etc, is the ability to get this speedily on a 24/7 basis.  
**Donald Toon**: I would certainly agree that we would have to retain the processes internally. The potential impact would be most crucially felt in those areas of investigation involving particularly large-scale organised fraud where the fraud moves very speedily. We see a series of organisations who will, for example, change the communication devices they use almost on a daily basis.

**Q166 Craig Whittaker**: Where speed is of the essence, do you think it is possible to devise a system that could distinguish between urgent and non-urgent cases bearing in mind a warrant system, if that was introduced?  
**Trevor Pearce**: You could design the system. The current system about direct and other forms of surveillance allows for urgency criteria. Of course, the answer is yes, and for all the right reasons we would want to work within those, but we would need to be reassured that the ability to act in situations of urgency and minimise bureaucracy in a time when we are clearly being asked to make significant efficiencies is important.

**Q167 Craig Whittaker**: If a system of prior authorisation was introduced, can you think of any particular permitted purpose for which authorisation should not apply?  
**Cressida Dick**: I am not sure that is a question for us, with respect. I am quite comfortable that in policing it is likely that anybody, having listened to the evidence, would think the reasons we use it now are the ones that should probably be retained in the future.

**Q168 Craig Whittaker**: Does anybody have a different view? What would be your view on the creation of some form of half-way house system with a level of third-party control falling short of a full warrant system, either in terms of the process to be followed or the cases in which such control was required? Do you have any suggestions as to how such a system might work?  
**Trevor Pearce**: The issues are security and safety of transmission, because this is, after all, data and we would need to be reassured that whatever the third party did and how they managed the process provided the same amount of scrutiny, information and assurance as you are seeking from us in terms of our current and future acquisition and usage. Security is a key issue, whether it is physical, technical or personal. That would need to be done, and the issue is availability and access, on which again we would want to be reassured.  
**Gary Beauchridge**: From my point of view, there are issues around what the capacity of that arrangement would look like and what the cost would be. To go back to what my colleagues
have said previously, if it was at all feasible I would urge on you a visit to look at the levels of professionalism and rigour applied to existing processes that, in my view, work very well.

Q169 Craig Whittaker: Do you think there are any authorities at all that should be put outside a warrant system?
Peter Davies: To clarify the question, I think we might be saying that a warrant system would not be necessarily appropriate.

Q170 The Chairman: Hypothetically, if there was a warrant system, are there authorities or public bodies that should be exempt from it?
Trevor Pearce: It is difficult to conceive of why there should be a different approach if the considerations are the same.

Q171 The Chairman: Let me ask a slightly different question. Mr Pearce, you quoted 240 urgent cases involving threat to life and kidnapping. Everyone on the Committee would accept that in those cases there is an urgent need to get information and pursue those with the utmost speed and rigour, but would you draw a distinction between a basket of cases like that and possibly tracking down paedophiles and pervers where sometimes you are years late on the case and there does not seem to be the urgency?
Trevor Pearce: There are two things: whether you have a reactive or proactive investigation. Significantly for us, where a large number of our investigations are drug-related, it is equally important to be able dynamically to go after numbers to enable us to identify and interdict a commodity of drugs before it hits the streets and our people become vulnerable.

Q172 The Chairman: Yes, but you draw a distinction between where there is a kidnap victim or threat to life and within 15 minutes you need mobile phone data and a case where 24 hours would suffice if you are chasing a known suspect.
Peter Davies: This is a distinction that is not uncommon in the exercise of a whole variety of different powers and procedures. There is the fast time and the slower time. Common sense dictates that there has to be the possibility of defining what is appropriate for fast time, for example a life at immediate risk, or loss of opportunity if it is not done very quickly. It is possible to make that distinction. It is analogous to other powers and processes, but I could not tell you exactly what it should look like in these circumstances.
The Chairman: I seem to have opened a can of worms.

Q173 Stephen Mosley: We have been talking about a warrant system before the request goes in. Would you have any thoughts on a notification process afterwards? If someone has had some sort of search done against their communications data, should there be a notification process in which they are told about it later, maybe with some sort of court process in there if, for some reason, you would not want them to know that because of an ongoing case?
Peter Davies: I am happy to follow up the previous point. I would not want you to assume that I think this is possibly the best way forward, but if you impose this kind of process the analogy is already there. Where people exercise powers in fast time there is a process of accountability to make sure the same scrutiny is applied, albeit retrospectively, because that is
necessary. I think the analogy carries through to that. It would be possible to have some retrospective scrutiny and powers exercised in extreme circumstances of urgency.  

_Cressida Dick_: At the risk of disagreeing with my colleague—I am sure we agree in some respects—there is a very high volume of cases involving long-term covert operations where we may or may not be successful in the first instance in bringing somebody to justice, and we would probably fight quite hard not to have to reveal the fact that they were targets, whether it is a counterterrorist or organised crime operation. I am no legal expert, but I think it would be a bit of a departure in our legal system.  

_Trevor Pearce_: We are perhaps speaking at cross-purposes here. Peter has been referring to, in cases where authority has been granted, whether you notify some kind of body, like the Information Commissioner, that that has taken place. That happens now in relation to Police Act and RIPA authorities with the Surveillance Commissioner’s Office. The other point of your question was: is the member of the public subject to that entitled to have information made available to them somehow that a request had been made? I think that is more challenging. Investigations ebb and flow and you may well compromise an investigation against that individual or others, and that provides a risk. In terms of this proposed legislation, there is discussion about the role of something like the Investigatory Powers Tribunal. In other jurisdictions this does take place. Talking to colleagues in other jurisdictions, they find it operationally challenging.

_Q174 Mr Brown_: I would like us to take up the suggestion of a visit to see particularly how the authorisation system works in practice. It would be a good thing for us to do. How much of a practical possibility is it to obtain information from the system improperly, either for personal use or just out of curiosity? Can operators do that, or would they be immediately caught and prevented from doing it?  

_Cressida Dick_: Practically, I think it is almost impossible. If you are the applicant, you have to apply with an intelligence case that relates to a real operation with real people and real data that you are seeking. The supervisor has to look at that and make sure that what you are asking for exists and is legitimate; likewise, the point of contact and the designated person. If you then ask whether the designated person or point of contact could do that, the answer is no, because there are different legs of the chair, if you like, all looking at each other and saying, “What is this case?”

_Q175 Mr Brown_: Is it a physical possibility to bypass that and get the information anyway?  

_Trevor Pearce_: I would suggest not. As our IT systems get more sophisticated, you can put in algorithms which will identify anomalous behaviour. We share all our information assurance practices to make sure we are able to carry out those sorts of audits. There is a range of protections from the application and authorisation process itself, the separation of those roles, the reasons for acquisitions and the technical measures in place to check for anomalous behaviour.  

_Donald Toon_: If you are asking whether it is possible theoretically, the answer must be yes, from my perspective, in relation to the designated persons who are the trained people authorising this. However, the systems in place would almost certainly ensure that if they did so they would do it once and would be caught immediately, because the cross-matching audit trail just would not exist.
Q176 Dr Huppert: To look again at the approach to warrants, we have looked at the issue of urgency versus non-urgency—I think we all accept there is a difference there—and the type of case. Clearly, a murder is very different from the speeding offences that Derbyshire’s chief constable seems to think count as serious enough to use this for. What about the option of separating it by the type of data? Some of you have indicated—I think it is true nationally—that most of the requests are for subscriber data, effectively reverse directory look-ups, which, to my mind at least, would be less intrusive than asking who somebody has rung over the last 12 months and exactly where they were when that happened. Would it be a possibility to have warrants only for the more intrusive types of request, for example, and to leave subscriber data requests under the current system? Would that satisfy many of your concerns?

Cressida Dick: Hypothetically, you could slice it different ways: urgency, certainly; seriousness, certainly; intrusiveness, certainly. You could try to slice it in all those ways, or in some combination of those. We believe that the disadvantages and disbenefits of that, given the strength of the current system, are very great and for us it would be difficult to justify going to that system, which would undoubtedly be a lot more costly and potentially burdensome.

The Chairman: This is fascinating. We are learning a lot, but we need to push on.

Q177 Lord Faulks: When I see the purposes contained in the draft Bill, they have their origins in RIPA. It is quite a long list. Criticism has been offered of the fact it is a long list and potentially puts the basis for obtaining information rather widely. I would like your comments as to whether you think it is too wide, and perhaps we can have assistance on which of the permitted purposes currently are most often relied upon. I do not know whether you have the list of permitted purposes available.

Donald Toon: I can give you a very quick answer. 99.5% of our requests are for the prevention and detection of crime; 0.5% are for the assessment and collection of tax or duty. That 0.5% was 69 cases in 2011.

Gary Beaumbridge: From the point of view of policing, primarily, it is for the purpose of preventing and detecting crime, or preventing disorder; secondly, it is for the purpose in an emergency of preventing death or injury, or any damage to a person’s physical or mental health. I have not got the statistics, but I could provide them to you.

Lord Faulks: Are the many additions to those core permitted purposes used regularly? Is anybody aware of them being used?

Trevor Pearce: Not from my perspective. I am sure others in the Home Office may be able to provide advice on that.

Q178 Lord Faulks: Should there be any difference between the types of data you can request and the appropriate authorisation system? There has been some suggestion that maybe there should be a distinction between, say, serious crime and non-serious crime, however difficult that is to define. Does anybody have any views on that?

Gary Beaumbridge: It is a matter of trying to define serious crime, which is very subjective, and it would be difficult to ensure any clear and unambiguous interpretation. Working with the Communications Capabilities Directorate, we are introducing systems across the country to retrieve data in a more consistent format. I think that will help the contextual understanding
of the overall situation and also reduce costs and the number of mistakes that may be being made at the moment, but it is subjective and ambiguous.

Q179 Lord Jones: Turning to misuse of data and monitoring, what level of monitoring and inspection occurs within your organisation to provide assurances to senior officers of the integrity of the SPOC process? How frequently has your organisation been inspected by the Interception of Communications Commissioner? How long did each inspection take, and what records were inspected on those occasions?

Gary Beautridge: The accredited officer role within our units is regarded as a gatekeeper. I have said previously that just over 20% of applications are declined by our single point of contact. Applications can be declined for a number of reasons: proportionality; collateral intrusion; and necessity. Once we have had a first look at the application, that goes on to a designated person. We also have refusals at that point. All of those applications are recorded in a system and are available for audits and inspection. We have an annual inspection by the Interception of Communications Commissioner. The last one concluded that the accredited officers were performing their guardianship roles and gatekeeper duties very effectively. In the last inspection for Kent and Essex, five recommendations were made. I could supply a copy of those recommendations to the Committee, should it think that would be useful.

Q180 Lord Jones: What lessons were learnt from the inspection, from the perspective of those who are giving evidence today?

Trevor Pearce: I do not have to hand the exact recommendations from our last inspection, but we are happy to share those with you and the action taken consequent on those. In addition to the range of management and supervisory responsibilities that go with this, as a non-departmental public body SOCA is also required to abide by the Cabinet Office guidelines in relation to information assurance, which itself is very rigorous. Having a senior information responsible officer within that process ensures that we look at the whole notion of how we manage our information and the assurance of it in line with the best practices that we report on once a year. In addition to the Information Commissioner looking specifically at either interception or communications data issues, we have oversight in terms of how we manage information more broadly.

Gary Beautridge: Inspections are very intrusive. They last three days. All records are looked at; officers and staff are spoken to about the different roles and responsibilities in this process. There is a very full report and debriefing that results.

Cressida Dick: The Met also has the Interception Commissioner there at least once a year. They come for a week or more in a large team. They are very intrusive indeed; they spend a lot of time with the staff, but they also examine a very high volume of records. I think that in our case it is getting on for 1,000 records they have looked at physically. They discuss their findings with us, including with an assistant commissioner, and make recommendations. Most recently, in our case they have identified some systems and administrative issues. They have also identified a couple of errors, which are useful to outline. Whenever we have an error that we ourselves find we must report it, and we do, to the Interception Commissioner. Then we must have an action plan about how we put that right. In the two errors they highlighted to us, we had sought more data than we had intended. The reason I give that example is that what the officers did was destroy the excess data straightaway. You might think that was the
right thing to do, but it is not what the codes of practice say, but they were so concerned about it they destroyed the data and immediately told the Interception Commissioner.

**Lord Jones:** The impression given is that you demand integrity and very largely, as far as you know, you are getting it, and integrity in the operations of your given departments is a huge priority.

**Q181 Lord Armstrong of Ilminster:** I know there are difficulties about defining serious and non-serious crime, but I think there would be people outside who would suggest that there are some non-serious crimes for which access to communications data should not be allowed. We were told that 17% of police communications data requests were for non-serious crime. It would be interesting to know whether other witnesses would report similar figures. If people were worried about this, would it be possible to devise a system which excluded the use of communications data in relation to non-serious crime, for example bicycle theft or something like that? If one said that one would not use this intrusion for non-serious crime, would that be workable? What do you think about it? I think this applies particularly to the police.

**Cressida Dick:** It is potentially workable, but I would give two caveats. Sometimes a crime that is in a category that appears on the surface not to be so very serious—I think I am right in saying that burglary does not feature in many descriptions of serious crime—can be extremely impactful and very serious for the victim, and may be part of a series in which we fear what might happen next. One can imagine circumstances—indeed, in the Met we sometimes do give authority in relation to burglary—where the degree of harm is so very high that we regard it now as a very serious crime, even though it is not in that category. To take the driving example Dr Huppert referred to, in the Metropolitan Police it is not unusual for us, after a fatal collision, to make communications data inquiries. I am sure that nobody would normally refer to that as just a driving offence—if there was an offence—but it will feature in that category potentially, under “driving”. Most members of the public would expect, if there has been a fatal collision, that we will check to see that the driver was not texting or on the telephone at the point of collision.

**Peter Davies:** As to the difficulties of defining what is and is not serious, one way of doing that is to look at whether the offence is triable only at a magistrates’ court or Crown Court. I will give you an example of why that is difficult. You may have heard of internet trolls who spend a large amount of their time inflicting serious psychological harm on people, for example through posting inappropriate messages or photographs on tribute sites to their recently deceased relatives. The appropriate offence for that is under the Malicious Communications Act, which is triable only at the magistrates’ court and is subject to time restrictions already. I think most people, certainly those affected by that kind of crime, would regard that as serious, and by its nature it is very difficult to investigate without communications data. I am not arguing for that to be included; I am merely observing how hard it is to draw a firm distinction between that which is serious and that which is not.

**Q182 Lord Jones:** Magistrates’ courts have been mentioned several times this morning. I think there are two: the district judge, the stipendiary, and the time-honoured three magistrates. Which would you prefer? Do you have a preference? Do you ask for one or the other?
**Peter Davies**: To clarify my answer, my point was more about the way the criminal law categorises malicious communications. I would not wish to express a personal preference, but colleagues may have a view.

**Q183 The Chairman**: Assistant Commissioner, you mentioned that in certain cases involving less serious crime one would need to check whether someone was texting or using a mobile phone on the motorway if there was a road accident. I confess an interest. Having been Police Minister, my admiration for the work of the police service is second to none. There are three constables in the Lords for whom I have tremendous respect: Condon, Dear and Stevens. Having said that, I am also cynical. Give the police a power for one thing and there is function creep; it gets extended to other areas. Within minutes of the Home Secretary at a press conference saying, “This is necessary for terrorism, paedophilia and serious crime”, Mr Mike Creedon said, “And of course if there’s someone on the motorway zooming along at 85 mph while texting, that is a threat to life, so we need to get that person, too.” Would you accept that it adds to the cynicism of some of those who are opposed to this Bill that, while we talk about terrorism, paedophilia and serious crime, there is a fear that if the police get this additional information it will be used to pursue other areas of crime that are not in that top-level category? It is an unfair question, but life is not fair.

**Peter Davies**: I was present at the press conference. My recollection of what Chief Constable Creedon said—he is not able to answer for himself here—was that it was in the context of using communications data to investigate fatal or serious road traffic collisions. That is an investigative staple. I appreciate and understand your point, but my understanding of what he was saying was more to do with the very serious consequences, which are to be prevented and avoided if at all possible, of people misusing communication devices while driving what are potentially lethal machines.

**Q184 The Chairman**: That was not quite my recollection, but let us not argue about it. What assurances can you give to prevent police function creep?

**Cressida Dick**: The assurance is how it is being used now, which we have discussed in some detail; the degree of seriousness with which we, as senior people, regard this; the systems we have in place; and the very proper safeguards in place, for example the commissioner coming to visit us. It is not for us to say what the police powers should or should not be and where they should be limited. I take your point entirely that intrusive powers should be used only when they are justified, and where that line should be drawn is a matter for Parliament. Rest assured, however, that, whatever we end up with, we will do our level best to ensure there is no creep. We will invite inspection and will be happy to have safeguards.

**Q185 The Chairman**: You cannot say fairer than that. ACC Beautridge, I was under the impression that the statistics you gave for Kent already covered the breakdown of serious and less serious offences. Why is a two-week snapshot necessary in the country if you and all the other forces are providing this information?

**Gary Beautridge**: We wanted to make sure a national picture could be presented that looked at the number of applications, what they were for and different categories of the applications so we could derive meaning from all the data out there at the moment. There was a huge
amount of data. The requirement for some analysis to derive some collective meaning is very important in the context of where we are, which was why we commissioned the study.

The Chairman: Thank you very much. We look forward to looking at the data from all the forces and the national snapshot, and we may come back to this. Assistant Commissioner and gentlemen, thank you very much. We have gone on longer than intended, but it has been very worthwhile.
Examination of Witnesses

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

Q186 The Chairman: Thank you very much for coming. Could you briefly state who you are for the record, starting with Mr Thornton?

Daniel Thornton: I am Daniel Thornton, Head of Legal in the Enforcement and Financial Crime Division of the Financial Services Authority.

Councillor Bettison: I am Councillor Paul Bettison. I am the lead member for regulatory services at the Local Government Association.

Gillian McGregor: I am Gillian McGregor, Director of Operational Intelligence in the UK Border Agency.

Nick Tofiluk: I am Nick Tofiluk, Director of Regulatory Operations at the Gambling Commission.

Q187 The Chairman: Thank you for coming. I am sorry we are starting slightly later than planned. We had a lot of information to collect in the last session. Can I begin by asking each of you some very brief starter questions? First, how often have you made requests for communications data in the past? Can each of you give us an answer, if you have it?

Daniel Thornton: As I understand it, we are the largest non-core authority in the use of communications data. I can give you the statistics for last year. We had 2,325 requests, of which about 65% related to subscriber data and about 35% related to more intrusive forms of communications data. Most of that was for the purposes of insider dealing criminal investigations, which is effectively an information crime, so it is all about the passage of information. That is why communications data form such an important part of our investigations.

Councillor Bettison: The Local Government Association is itself a membership body. Therefore, we never request communications data directly as we have no requirement so to do. Our individual member councils, however, can currently request communications data but only for the purpose of preventing or detecting crime or preventing disorder. These crimes are often targeted at the most vulnerable in our communities, and can include rogue traders, loan sharks, doorstep crime, antisocial behaviour, environmental crime, animal welfare issues and benefit fraud. The LGA does not itself collect data on the number of requests for communications data; we leave that to the Office of the Interception of Communications Commissioner. The annual report from the commissioner’s office indicates that all requests received from councils make up only 0.3% of all data requests. We believe this low figure shows that councils are exercising their powers in a proportionate way and requesting data only when absolutely necessary.

Gillian McGregor: In 2011, the Border Agency made 4,062 access requests. The Border Agency figures are included within the general law enforcement and security agency figures in...
the IOCCO reports. That is an increase on 2010 when we submitted 2,854 requests. We anticipate that this year the figure will be higher, which reflects the fact that the agency has taken on a much more central role in the investigation of serious crime in relation to immigration and border issues, such as drugs importation, facilitation and trafficking.

**Nick Tofiluk**: Because the numbers are so much smaller for us, being a relatively small organisation, we made 104 applications over the last three years, which averages 35 a year. That resulted in 636 requests, of which 68% were for subscriber data, 24% for user data and 8% for traffic data.

**Q188 The Chairman**: I think each of you has told us what types of data you have tended to request.

**Gillian McGregor**: I do not think I did. To clarify it, our breakdown is that for subscriber data it is about 70%; for service use data it is 5%; and for traffic data it is 25%.

**Q189 The Chairman**: Under which permitted purpose in RIPA have most of your requests been in the past?

**Daniel Thornton**: All of ours have been for preventing and detecting crime because they have been for the purposes of criminal investigations. To put a slight gloss on that, one of the new permitted purposes under this draft legislation is civil market abuse, which we also investigate, where we can impose a civil penalty. Those powers arise under the Financial Services and Markets Act and come from a European directive. The proposal in this legislation is that, instead of using that power, the power is streamlined under RIPA, or RIPA-type processes, to use the same sort of process. We adopt exactly the same processes using our FSMA powers as we do when using our RIPA powers. That is the breakdown of how we use it under the Act.

**Councillor Bettison**: All of ours are and will be for the prevention or detection of crime or preventing disorder.

**Gillian McGregor**: For the Border Agency, over 99% are for the purposes of preventing and detecting crime. A very small percentage is related to our statutory responsibilities for detention services. That is related to public safety for the maintenance of good order and discipline on the detention estate, but also prevention of escape and riots.

**Nick Tofiluk**: The prevention and detection of crime.

**Q190 The Chairman**: For what kinds of investigations, as far as you can tell us, do you use the communications data?

**Daniel Thornton**: Most of it relates to insider-trading investigations, principally about someone trading on the basis of inside information. There is often quite a long distance between the inside source and the person who is dealing. It is a form of organised crime. We see groups or rings of people who pass data between them, and therefore communications data is key to trying to work out the connections between the person who traded and where the inside source is. That is probably the principal means for which we use this data.

It also is important for market manipulation, for example people posting messages on bulletin boards to try to move a stock price and then trading on the back of that. That is one of the abuses we have seen. We also use it in the unauthorised business area; that is, people who are trading without authorisation, which is effectively a form of fraud, in that they are selling worthless investments to vulnerable consumers. We use that often to try to be sure who is
calling the consumer. For example, a lot of these people will use false names, so often it is important to try to work out who is making the call. We have also used it in a similar investigation to track down from where a boiler room was operating. That is a group of criminals pressure-selling worthless investments. We used that to locate where they were operating from using internet data, for example, and executed a search warrant at the right premises.

**Q191 The Chairman:** Councillor Bettison, you gave us some examples. Could you rank them in order of the most used?

**Councillor Bettison:** Probably, these days most of the use relates to benefits fraud. We know that the Government’s message to benefit fraudsters is, “It’s not if we catch you but when.” Certainly, the use of these powers assists us to help the Government make good on their promise.

**The Chairman:** I presume that would be housing benefit at district rather than county council level.

**Councillor Bettison:** That is right. As Mr Thornton has said, it is often very much a question of tying in somebody who has given a false name, or no name, in a communication with someone. It is certainly in the realm of rogue traders as well. That is another very large use, bearing in mind how little we have to resort to it. But in those cases where we do have to resort to this sort of information, it is absolutely vital. I have a number of case histories, which I would be very happy to supply in writing if that would be useful, where conviction has been possible only by this type of information being available.

**Q192 The Chairman:** Would you be able to give us an assurance that some of the cases we have read about will no longer occur, such as check-ups being made on a parent as to where they live and the area in which their child goes to school, or whatever, which would seem to be an abuse?

**Councillor Bettison:** We are very conscious that, due in no small part to the activities of the national press, these very rare occasions make much bigger stories. The reality is that the public, therefore, need reassurance. That is why we are very happy indeed to continue to work under the extremely stringent regulation we have to abide by in order to access this information.

**Gillian McGregor:** In the Border Agency we use communications data for quite a wide range. If I was to rank them as you request, the most common use would be in relation to drug smuggling and the smuggling of prohibited items. That is a matter the agency is responsible for, and our customs colleagues have joined us. There is also facilitation and organised people smuggling; trafficking offences; bonded labour; vice, or vulnerable persons, including children. We also use communications data for other immigration offences, such as the use of forged and counterfeit documents and organised crime groups that might be involved in that sort of activity; and sham marriages and bogus colleges. There are a number of different things, but I would suggest that is the kind of ranking for which communications data would be used.

**Nick Tofiluk:** In the case of the commission, 79% of our applications are focused upon the offence of cheat. If I can put that in the context of something that is perhaps more recognisable—match-fixing and all that that entails—the commission is the lead for the
intelligence function with colleagues from ACPO, sports governing bodies and betting operators to address this threat. That involves the corruption of betting markets and the facilitation of those prepared and able to manipulate sports events as well as betting events, predominantly online betting. It also involves the use of inside information, so there is a lot of similarity with my colleague from the FSA. 17% of our applications have been focused on those illegally supplying gaming machines, which is a very lucrative pastime, if I can call it that, or enterprise, to premises that are possibly unlicensed for such. It has not only a criminal aspect but also relates to the commission’s objective which is preventing harm to children, young persons and the vulnerable, which we think is very important. 4% relates to the unlicensed provision of gambling services. It is very much weighted in terms of match-fixing.

Q193 The Chairman: That is very helpful. My final starter question is: you have all pointed out that you are very low users. Why are you not using it a lot more? Gillian McGregor, the Border Agency realises that it has a powerful tool here. You are going to double the intake, or the requests.

Gillian McGregor: We are making use of these powers daily, and our use is increasing. I gave the figure of 4,062 (individual communications data items) in 2011. We are projecting that for this year our figure will be in the region of 6,000 individual communications data items, but we have to make sure that what we are requesting is proportionate and necessary. I think it reflects the balance between our central role as the law enforcement agency for this type of crime and the proportionality of what we are doing. We also have a very close relationship with other agencies, such as SOCA and ACPO, and on some occasions our investigations will be so serious that they will be elevated to those agencies.

Q194 The Chairman: Is the proportionality hurdle for you in some ways too high? Are you being judged against the same yardstick as the security services in dealing with terrorism or the police in people trafficking and paedophilia? Do you have to show the same level of proportionality in chasing illegal immigrants as our security services do in chasing terrorists?

Gillian McGregor: The elements of proportionality are similar, because lots of the investigations we are dealing with are on a par with some of the serious cases that the police and SOCA investigate. Our judgments on proportionality and necessity are similar.

Q195 The Chairman: Do any other witnesses wish to comment? Do you feel constrained? Would you like to use them a bit more if you could?

Nick Tofiluk: I echo that to a very great degree, and I think it follows on from the previous discussion about what we mean by “serious”. Towards the latter part of the previous session the word “harm” started to feature in the discussion. From the commission’s perspective, the licensing objective is very much focused upon harm, and I would want us to start to think about harm in terms of children, young persons and vulnerable people being exploited by gambling, and then fairness. For us, proportionality is a combination of the criminal impact and the wider harms. The commission has 200 staff in total, and therefore the ability to use the powers wisely in terms of resource efficiency, as well as our ability to use the data once we have got it, is constrained, but, as my colleague from UKBA has said, increasingly we work in collaboration on the more serious cases with police forces and HMRC, and because of the global nature of gaming and sport we are increasingly engaged in international collaborations.
Q196 Lord Jones: On the future use of communications data, none of the bodies on the panel here today is on the face of the draft Bill. This means that if you are to have access to the data you have to be added by order under the parliamentary process. Do you wish to have access to communications data in the future, and have you been given any assurances that you will be added?

Daniel Thornton: We are not on the face of the Bill, although one of its purposes, to combat civil market abuse, is an offence that only the Financial Services Authority can pursue, which could be said to be a slight contradiction. The reason for it being there is that it is in European law in the form of the Market Abuse Directive. We think we have a very strong case to have these powers. Whether that is on the face of the Bill or through a statutory instrument does not make any difference to us per se. We have to go through a process to get approval from the Home Office, but ultimately how that is done is really a matter for Parliament.

Councillor Bettison: Clause 11 of the draft Bill and the recent Protection of Freedoms Act provide councils with the power to continue to access communications data with the approval of a magistrate. We believe this shows clear recognition by government of the importance of these powers for councils to protect their communities from crime. However, since the Bill was published the Home Office has advised the LGA that it is expected to make a business case for a specific order to ensure that councils can retain access to communications data. The changing stance, along with differing legal views about whether the order is required, has created significant confusion and concern about government intentions on the matter. It would be helpful to have a clear message from government to support the importance of councils retaining access to communications data to protect the most vulnerable parts of their communities from crime, and to acknowledge that councils are making good use of current powers in a wholly proportionate manner—witness the very small number of uses currently.

Lord Jones: Thank you for the information as to what the Home Office has said to you.

Gillian McGregor: The Border Agency is not on the face of the Bill, and that reflects the position in RIPA where our powers come from secondary legislation. Things have moved on for UKBA. We are recognised as a law enforcement partner with a very clear role. We want to retain access to communications data. Like my colleague Councillor Bettison, we have been asked to produce justification for that continued access. Similarly, the most important thing for us is to retain access to communications data. Whether that is through being named on the face of the Bill or through secondary legislation is possibly a secondary issue, but we want to retain access.

Q197 Mr Brown: Is it true for the FSA and the Gaming Commission that they have been asked to prepare for draft secondary legislation?

Daniel Thornton: We have been asked to provide data to the Home Office and present a business case as to why we should have access to communications data.

Mr Brown: Is that so for the Gaming Commission?

Nick Tofiluk: Yes.

Mr Brown: Why do we not seek a list of the organisations that have been asked to prepare for this eventuality? In other words, tell us something we do not know.
Q198 The Chairman: I agree entirely. We shall request that. What is your deadline for producing your business case? Are they all roughly the same?
Daniel Thornton: We are supposed to produce some data by 20 July.
Gillian McGregor: Yes; it is the same for us.
The Chairman: You are required to produce data, a business case and justification for having an order made in your favour.
Gillian McGregor: Yes.
The Chairman: You have to produce that evidence, data and justification by 20 July to the Home Office.
Daniel Thornton: That is right.
The Chairman: That is helpful.

Q199 Lord Jones: Can you tell us briefly what would be the implications for you if you did not have access to the data you want?
Daniel Thornton: That is somewhat speculative, but certainly with insider dealing many investigations would not get anywhere; it simply would not be detected. We would see suspicious dealing but would not be able to identify whether or not it was innocent. In most of our criminal insider-dealing prosecutions, communications data has formed a central part of the evidence. As it is about the passage of information, it is an offence that you prove through circumstantial evidence. One of the most important parts of circumstantial evidence is the timeliness of communications and who was calling whom. The insider calls somebody who then calls somebody else who then calls the dealer who immediately places a trade, for example. Showing that pattern of behaviour and calls is absolutely central to most of our prosecutions. If we did not have access to this data at all, it is likely that many crimes we currently prosecute we would not be able to prosecute at all.

Q200 Lord Armstrong of Ilminster: Do you think you ought to be on the face of the Bill? Would you prefer to be on the face of the Bill?
Daniel Thornton: I would prefer not to have to make a business case, if that is what it means.
Lord Armstrong of Ilminster: You might have to do that either way.
Daniel Thornton: Yes. As colleagues have said, for us the important thing is to have the power. Exactly how it is portrayed in legislation is really a matter for government and Parliament.

Councillor Bettison: I think that not to allow local authorities these powers would leave councils without the necessary tools to protect their residents and businesses and seriously undermine the Government’s message to benefit fraudsters: “It’s not if we catch you but when”. There have been a number of high-profile cases where benefit fraudsters have been identified, caught and dealt with. It is important that people understand that benefit fraud is not an easy way to win on the system, and to make sure they cannot.

Q201 Lord Jones: In your experience in local government, are there many benefit frauds? Is it very serious?
Councillor Bettison: That particular fraud is stealing from everyone, and if we are not careful it could become one of those victimless crimes, simply because we cannot identify everyone,
because as taxpayers we are all victims of those crimes. It is very important that councils are seen to have the ability to find out if people are cheating the system and stop them doing so.

**Q202 Lord Jones:** Would your business plan include evidence that there are many cases?

**Councillor Bettison:** It would include the details such as we have of the magnitude of the problem, and also examples where the problem has been dealt with by the use of this data communications information.

**Gillian McGregor:** Similarly, if the Border Agency did not have access to this data it would seriously hamper our ability to investigate immigration and customs crime, particularly serious ones. The crimes we are dealing with are international, fast-moving and involve communication across borders, so we rely heavily on communications data. To give you a flavour, in 2011 we conducted 461 separate criminal investigations that involved access to communications data.

**Nick Tofiluk:** If I may return to the previous question, because I did not answer, we expect to be included on the list, and I would be extremely disappointed if we were not. I would be less bothered about whether that was by statutory instrument or on the face of the Bill. We were given powers for criminal prosecution under regulation, and I think that is totally consistent with what is expected of us as the core purpose of the Gambling Commission. If you think of our core purpose as regulating the gambling environment, a large proportion of it is now moving to a remote base. The global gross profit of remote gaming is increasing year on year. The second part that makes the case for me in terms of our regulatory and associated functions, possibly policing functions, in that environment is that perhaps in two years’ time the licensing arrangements for those providing remote gambling to UK citizens will change. We will have to license those at the point of consumption, or what is provided to UK citizenry—presently we do not have to—which is likely, in my estimation, to increase five to six-fold the market in gross profit terms. Therefore, being able to understand and retrieve data from a remote environment, where the scale of gambling and the technology that supports it is fast-moving, is absolutely critical. In terms of our role in the lead for sports betting corruption and match-fixing, without the powers given to us under RIPA I do not think we would be able to perform that role.

**Q203 Michael Ellis:** Councillor Bettison, local authorities currently cannot request traffic data from service providers, whereas other bodies represented here can. The draft Bill replicates that limitation as far as local authorities are concerned, and further states that local authorities will be able to request only information that service providers continue to generate out of business need. This may be the result of a perception in some quarters that local authorities have been responsible for frivolous applications. I would like to give you the opportunity to say whether you think this limitation poses any problems for local authorities. Can you make a case for wider access?

**Councillor Bettison:** I am sure that, given due warning, we could make a case for wider access, but the Local Government Association itself does not collect data on actual use of data.

**Michael Ellis:** I accept that, but can you speak behalf of the local authorities you represent?

**Councillor Bettison:** As to whether or not we could use additional data, I am sure we could find cases where it would have been useful. Having said that, I am here today quite content with the powers that we believe are being offered to us and am not demanding greater powers.
I would look for any assistance in dispelling any myth about our limited powers being the result of frivolous activities in the past, because I do not believe that to be the case.

**Q204 Michael Ellis:** I think I am right in saying that the other bodies represented here can request all types of communications data, including traffic data. For each of you who can, how often do you request traffic data, and in what kind of investigation is traffic data most useful?  
**Daniel Thornton:** The first stage is often to get the subscriber data to work out who is calling whom, but traffic or use data is essential to work out the timing and length of telephone calls, for example. In some investigations, it has been important to work out where people are at particular times, or when they are logging on to, say, a secure internet site being used to deposit information. Our usage is probably between 30% to 40% per year for the more intrusive forms of data, apart from subscriber data.  
**Gillian McGregor:** The agency relies heavily on traffic data, so it forms about 25% of our data requests. I think the cases to which it is particularly relevant are trafficking, facilitation and smuggling offences where, like my colleagues, it is important to be able to be aware of movements, to know who has been talking to whom and how that is progressing. If it would help the Committee, we would be very happy to share examples of cases where traffic data has been particularly helpful in achieving a conviction.

**Q205 Michael Ellis:** Indeed. Could you give one brief example now?  
**Gillian McGregor:** Yes, I could. We dealt with a major investigation into a serious organised crime group operating in Manchester, which was importing drugs. For that particular investigation we used a mix of all the different types of communications data, including cell site data, through which we were able to track the movements of suspects, and, linking that with other information, we placed them in a position where we understood they were people operating the organised crime group. To give you the scale of the operation, it involved class A drugs—heroin—one of a total weight of 175 kilograms with a street value of £13.5 million. The two main members of the organised crime group were sentenced respectively to 11 and nine years in prison, so traffic data was very important in that particular case.

**Q206 Michael Ellis:** Is it important to the Gambling Commission?  
**Nick Tofiluk:** Very, and in almost exactly the same circumstances as my colleague from the FSA described. What we are trying to do is prove connectivity between facilitators who can influence sporting events, not just the result but incidents within them, and the placing of bets and communication between those people who are connected in that type of manipulation of the market.  
**Michael Ellis:** Is it right that those of you who can utilise traffic data at the moment feel you need it, and you would be at a serious disadvantage if you were restricted in the same way local authorities currently are?  
**Daniel Thornton:** Yes.  
**Gillian McGregor:** Yes.

**Q207 Michael Ellis:** What percentage of communications data do you feel you need for your own investigations that is no longer available? We have heard about a degradation from 95% to 100% many years ago to 75%. Can you say something about how lack of this data has
affected your investigations? Do you agree there is no longer as much access to data, for whatever reasons, as there used to be?

**Daniel Thornton:** It is very difficult to say. In our investigations we get quite close to the 12-month time limit because of their complexity. It is rather like an onion; you are peeling layer after layer to work out the connections, and by the time you get to where you want to be you are hitting the end of the period for which we know telecoms companies keep material. That is a definite limitation. What we do not know is the extent to which more sophisticated means of undetectable communication are being used at the moment. In our investigations we are seeing more sophisticated techniques being used, for example pay-as-you-go mobile phones but also self-destruct USB sticks to store sensitive data, which are passed between people, and the use of secure internet sites as a way of passing information. The people we are tracking are becoming more sophisticated in their techniques.

**Michael Ellis:** Self-destruct USB sticks?

**Daniel Thornton:** These are where you have hardware encryption, so if you enter the wrong password three times it destroys the data.

**Michael Ellis:** It is not like “Mission Impossible”.

**Daniel Thornton:** Almost.

**Q208 Lord Faulks:** Do you think that the ability to access communications data reduces the amount you would otherwise be spending on investigations? In other words, is access a significant cost benefit, or not?

**Daniel Thornton:** I find that a very difficult question to answer. It is a unique and central tool, so it is not a question of having an alternative technique to get the same information. The premise of the question does not really work for our sorts of investigations, because you simply would not be able to detect the connection rather than have an increased cost to try to find it.

**Nick Tofiluk:** From the commission’s perspective, the position is similar in the case of looking for organised crime related to match-fixing and insider information, but, in the case of what you might call bricks and mortar-type investigations, the consequence may very well be that our only real alternative would be to use some form of directed surveillance, which would possibly add tremendously to the cost. I have personal doubts whether it would be that effective, and it might be even more intrusive than our current mechanisms.

**Q209 Lord Faulks:** More costs in terms of manpower.

**Nick Tofiluk:** Absolutely.

**Gillian McGregor:** For the Border Agency it is quite difficult to quantify, but there are two angles to this in terms of cost. One is very similar to the point made by my colleague from the Gambling Commission. If we did not have access to this communications data, we might need to consider more resource-intensive direct surveillance activity, which would be very time-consuming and costly. We would also have to consider carefully whether we investigated certain serious crimes.

**Lord Faulks:** Because you did not have the resources.

**Gillian McGregor:** Yes. That brings its own cost in terms of both the cash seizures that might follow a successful prosecution but also the general cost to UK plc as a result of increased
crime. We can attempt to do that if the Committee would find it helpful, but it is quite difficult to quantify.

Councillor Bettison: We do not carry data on that, so I am not able to assist.

Q210 Lord Strasburger: All the discussion so far has been about the use you make of data obtained under RIPA and your desire not to lose access to that, but you will be aware that this draft legislation substantially expands the range of data that would be available to public authorities. Is there any of that expanded data, and if so, which, that you feel would improve the ability to do your job?

Gillian McGregor: My view would be similar to that of my colleague from the FSA. We do not know what we do not know, but our sense is that the serious criminals we are dealing with on the immigration and customs side are making increasing use of more sophisticated internet and smart phone techniques to communicate. It would potentially give us more options, but the same considerations of proportionality and necessity would apply. The agency is looking to retain the ability to keep up with the communications used by the criminals we are dealing with, and we understand that because technology is progressing the current information is perhaps not the whole story.

Nick Tofiluk: I agree with the point about the sophistication of those we are trying to find in disguising their footprint, but from the commission’s perspective we are entering an era where the remote gambling platforms are of increasing sophistication, not least because of what we call peer-to-peer gaming. A global internet room means that communication is taking place not only through different technologies but over international boundaries. We are looking at the potential for things like money-laundering through techniques that enable peer-to-peer gambling, or playing through exchanges. In one sense we do not know what we do not know yet, because we are in a process of discovering exactly what techniques are being used to pass information, what technologies are being used and what the fundamental difference is. This is going to pose as much of a challenge for us to define what it is to CSPs, so they are on the lookout for it, as it is to describe it to ourselves to capture it. From the perspective of the Gambling Commission, a period of dialogue is coming, possibly through the engagement of ACPO’s Data Communications Group and the CSPs, about the exact nature of the information now being transacted in what can broadly be called fraud through gambling. We would start by needing to define “capture”.

Q211 Mr Brown: I want to return to the point about warrants. Councillor Bettison, are you able to tell us what proportion of warrant applications are rejected by magistrates?

Councillor Bettison: No, but I am sure that we would be able to come back.

Mr Brown: Would you be able to supply that to the Committee?

Councillor Bettison: Yes.
and work in a secure area. They are the first gatekeeper, if you like, for applications. The designated persons are heads of department in the Enforcement and Financial Crime Division, who are well used to managing complex financial services investigations and judging proportionality and necessity, which they have to do in their daily jobs in respect of how we exercise our statutory powers more generally. This is not the only intrusive power we have into data. That is how they fit in. The senior responsible officer is me. There are also lawyers involved in a lot of the steps in the process. We have lawyers in the investigation teams. The SPOC is looked after by a lawyer who assists in any legal issues arising. The majority of our heads of department are also lawyers and I am a lawyer. We are probably a bit lawyer-heavy, but there is a great deal of legal oversight in the whole process.

**Lord Armstrong of Ilminster:** Are your senior designated officers sufficiently detached from the individual cases?

**Daniel Thornton:** Yes. You cannot be a senior designated officer on a case you are managing or are involved in, so there is independence from the investigation that is being conducted.

**Q213 Lord Armstrong of Ilminster:** Councillor Bettison, this may be a difficult one for you. **Councillor Bettison:** It is perhaps slightly different. Because of the level of data requests submitted by individual councils, it would not be feasible to have an officer dedicated solely to approving requests for communications data. Senior officers, although still an integral part of the service or legal support associated with the detection and prevention of crime, are required by RIPA to be designated officers, and their standing within the local authority is that of a director, head of service and service manager. All RIPA-style activity is also overseen by elected members. As responsible employers, all councils ensure that these individuals are very well trained, although it is not their sole purpose in the authority to do this, as I mentioned earlier. We take it very seriously, and, in the final analysis, the elected members are responsible.

**Q214 Lord Armstrong of Ilminster:** Presumably, the number of designated officers will vary according to the size of the authority.

**Councillor Bettison:** In most authorities it would be one.

**Daniel Thornton:** For us, it is seven.

**Gillian McGregor:** The Border Agency has an arrangement very similar to that of my colleague from the FSA. We have a single point of contact, which is a very small secure unit that processes all the requests. They are referred to the designated senior officers, of whom we have 18 across the whole agency. It is a relatively small number for an agency that employs thousands of people. They are all people who are regularly involved and highly trained in investigations under RIPA, but, as with my colleague, there is a very clear dividing line. An application that could be considered by the senior officer must not be an investigation in which they are involved. We find that quite easy to manage. Our agency is based nationally, so it is very easy to separate the investigation from the designated senior officer who would approve or otherwise the request.

**Nick Tofiluk:** The commission is very mindful that you might be involved in the war but the rule is that you are not involved in the individual battles. We have two fully trained single points of contact within the secure intelligence environment. They are trained by the National Policing Improvement Agency and accredited to the same standards as the police. We have
four designated senior persons, one of whom is not the head of enforcement, to enforce that separation. All are trained, and three of those four have previous experience either with SOCA or the police and have gone through training there and have had responsibilities in those environments. The senior responsible officer is myself, and the unit is led by the head of intelligence, which has responsibility for wider information management as well as RIPA.

Q215 Stephen Mosley: You have been talking about internal monitoring. From the external point of view, can you talk about the process of the Interception of Communications Commissioner that you have seen?

Daniel Thornton: We have had several visits, probably every 15 to 18 months. One of his inspectors comes for two days, does a very thorough review and looks at many requests. We have always come out well from our inspections, in that all the applications looked at have been lawful, proportionate and necessary. We see it as a very thorough process.

Q216 Dr Huppert: I declare an interest as a vice-president of the Local Government Association. I am struck by what we have heard already. Despite the focus and rhetoric on how powers to access data will be reduced to four key organisations, it seems that you have all had discussions with the Home Office about expanding it again. I can see how these things balloon. On the face of the Bill, the Local Government Association is in the rather odd position of not being included but having constraints on the powers it could exert if it was to be included, whereas the rest of you are just not in the Bill at all. Do you support the fact that the warranting system was introduced? Are you concerned that it might put off local authority officers from requesting data?

Councillor Bettison: We are not concerned that they would be put off requesting data. They request data so infrequently that it is already of such importance, and if that is the price we need to pay we will pay it.

Dr Huppert: You support the warranting system.

Councillor Bettison: Yes.

Q217 Dr Huppert: That is very helpful and clear. The rest of you are in the odd position of not being included on the face of the Bill but also not having any constraints. Given the relatively small number of data requests you all make, it seems that, like the Local Government Association who accept the warranting system, that could be made to work for you as well. Would you be comfortable with such a system?

Daniel Thornton: I do not accept that. The volume of our requests is quite significant. To introduce a warranting system, even if it was for only the more intrusive forms of data—i.e. not just subscriber data—would be quite a significant change from our processes. You can judge whether or not it is necessary in terms of the robustness of our processes, but to have to go to a magistrate means it would probably be at least once every working day for the amount of requests we are putting through. It would be quite a considerable burden. Our other significant concern about introducing that sort of system is the likely delay caused to investigations. We are not dealing, except in exceptional cases, with very urgent applications. It is not like going for a search warrant, for example, which can be done in a few days. These might get to the bottom of the pile. If they are going to take weeks, there is a danger of significantly prolonging the investigations and our being unable to get access to data at all,
because it will drop off the end of the 12-month period, not to mention the cost and expense of this sort of process. It is not like we would be doing one a month; it would be much more frequent.

**Dr Huppert:** Any system would have to be prompt and efficient for it to work for you.  
**Daniel Thornton:** Yes.

---

**Q218** **Dr Huppert:** What about the other two agencies?  
**Gillian McGregor:** I would completely echo what my colleague from the FSA said. We have similar issues. Our volume of requests, although a small percentage—it is about 1% of the total—is still quite a significant number. We would find it very challenging to operate the warrant system in terms of the capacity and cost that might be involved, but also there would be potential delay in cases. A number of our cases—not all—require a response to very urgent situations, including high-harm subjects and, in certain circumstances, a risk to life, for example trafficking cases, or dangerous people who have breached the border.  
**Nick Tofiluk:** Our volumes are relatively low, and, therefore, I would not be in the same position as colleagues who have spoken already. There would be a cost implication for us in terms of a small organisation. The issue of delay would be a concern to me, although we are not in the territory of threats to life, but again we would, more than likely, go a court in the centre of Birmingham, which may very well be having a lot of other requests given the nature of the city and other organisations in that area, so there is the issue of delay. I would ask what value that would add, not least because, as colleagues said in the previous session, we would retain our internal scrutiny and oversight. I am not questioning the principle, if that is the wish.

---

**Q219** **Dr Huppert:** Do you all accept there is a fundamental issue about self-authorisation for powers versus external authorisation? You are presumably aware that almost every other country with a similar process has some form of third-party authorisation. Do you accept that principle at least?  
**Nick Tofiluk:** There is a question about transparency and whether we have faith in the oversight arrangements at the present time. That is not for me to answer in that sense. If it is the will of Parliament that there is transparency through the courts, quite rightly that would be accepted, but, as police colleagues also said, that would not mean our internal arrangements would be any the less robust.

---

**Q220** **The Chairman:** When the new National Crime Agency is set up, will UKBA become part of it, or does part of UKBA link in with it in pursuing investigations?  
**Gillian McGregor:** The agency will remain separate. We are part of the Organised Crime Partnership Board with the police, SOCA and HMRC, so we are very closely linked with the National Crime Agency. There will be a border policing command aspect to the National Crime Agency, but the UK Border Agency will remain a separate organisation.  
**The Chairman:** That is helpful. You have clarified what I imagined was going to happen. Thank you very much. I am sorry we are running slightly late. We have had an excellent evidence session again, and we very grateful for the information you have given us.
TUESDAY 17 JULY 2012

Members present:

Lord Blencathra (Chairman)
Lord Armstrong of Ilminster
Baroness Cohen of Pimlico
Lord Strasburger
Mr Nicholas Brown
Michael Ellis
Dr Julian Huppert
Stephen Mosley
Craig Whittaker
David Wright

Nick Pickles, Jim Killock, Rachel Robinson and Angela Patrick (QQ 221-274)

Examination of Witnesses

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

Q221 The Chairman: Welcome to our fourth public evidence session. Welcome to Mr Pickles, Mr Killock, Ms Robinson and Ms Patrick. For the record and for the benefit of the public, who may wonder what is happening, Mr Pickles and Mr Killock were giving evidence last week. We did not manage to get through all the questions that we wanted to ask of them, so we have added them to today’s session. However, we will ignore them for the first few questions, because we have a few questions we would like to put to Ms Robinson and Ms Patrick first, if we may. Could I start, therefore, by asking you—Ms Robinson and Ms Patrick—to outline your main concerns about the proposals embodied in this draft Bill? What are the areas that you each hope this Joint Committee is going to consider?

Rachel Robinson: I will make a start. Liberty is of course incredibly concerned about effective law enforcement, and particularly the need to protect the public from serious harm. We have never opposed targeted surveillance based on individualised suspicion, but what we have here is really a far cry from that. We have concerns about all areas of the Bill, but really the core of our concerns and the fundamental shift here flow from Clause 1 and from arrangements for collection of communications data. Communications data is already unique in terms of its historical availability to law enforcement agencies. While other countries across Europe are challenging the constitutionality of arrangements as they stand, we are finding ourselves in the position of pushing for a real sea change, a real step change, in terms of the arrangements for collection of communications data. Never before have private companies been called upon to collect data, which they have no business purpose to collect, purely on a just-in-case basis to satisfy potential future requests.
We hope the Committee will explore what we identify as the three fundamental assumptions - and flawed assumptions - upon which this policy is based. Firstly, there is the idea that communications data is, in some way, not particularly intrusive or not particularly revealing. We argue that is incredibly revealing in the current technological environment. Secondly, there is the idea that it even makes sense to draw the distinction conceptually between communications data and content. Thirdly, there is the idea that law enforcement gains would seamlessly flow from these provisions. We would suggest that the law enforcement case is, at best, shaky and incomplete. We hope the Committee will have an opportunity to examine these assumptions.

Q222 The Chairman: Thank you. We will wish to come back shortly on your assertion that countries across Europe are challenging it, but I did not want to interrupt the flow just now. Ms Patrick.

Angela Patrick: This is all going to sound very familiar now you have heard from Ms Robinson, Mr Pickles and Mr Killock, but Justice has worked on these issues for decades. We first reported in the 1970s that we were really concerned that we were racing headlong into a society where technology was advancing so quickly that our privacy laws were not keeping pace. I am new to my organisation, but these arguments are not new to us. We would like to begin by saying that Justice recognises that surveillance, in many cases, is essential for the purposes of the prevention and detection of crime. In many cases, the work of the police, law enforcement agencies and the intelligence services saves lives. We accept that, but actually the flipside to that is surveillance is of a particular nature. It is accepted by everyone that, by its nature, it imposes restrictions and interferences on individual privacy. This is of different degrees of severity, but the starting point is that it does engage our individual right to privacy, as it is protected not only in the European convention but in the principles of our common law that stretch back centuries.

Those are the two flipsides with which we would like to start off the Committee: surveillance is legitimate, but it does engage privacy and needs to be justified; and surveillance, by its very nature, in order to be effective has to be covert. When looking at the regulation of surveillance, it is particularly important for parliamentarians to be aware of the need for effective controls and safeguards to ensure that surveillance is only used in those circumstances where it is strictly necessary and justifiable. Individuals in most cases, if surveillance is effective, will never know that it has happened and so will never have access to an effective challenge or a remedy. That is our starting point.

Moving to the Bill, and I will be very brief because I know we have specific questions, I would like to put down three markers. Our first is that there is so much uncertainty in what this Bill is asking for that it is impossible for us, as civil society commentators, to pick it apart in terms of trying to help you, as parliamentarians, understand what the real risks are and what the challenges are for the Government in terms of providing evidence. It is so open, in Part 1 of the Bill, that I am finding it quite difficult to range our concerns, let alone ask what the right questions for you to ask are. Actually, when you are starting from a premise that what you are doing is engaging individual rights, that is really worrying. The Joint Committee on Human Rights has routinely called upon the Government, when they are looking at legislation that engages individual rights, to provide information to allow parliamentarians to conduct proper
scutiny. That Clause 1 of this Bill is so broadly drafted must be the first concern for this Committee, we would submit.
The second is, to reiterate Ms Robinson’s concern, this is not about data access alone; it is about data collection. Your first 101 lesson, as a lawyer being told to understand the law on privacy, particularly as it applies to the European convention, is that every use of data is a new and interesting issue or set of circumstances, for which you have to look for justification. Here in the Bill, your starting point is: is the new proposal on collection of data justified? Is the proposal on collection accompanied by appropriate safeguards? Are the measures for retention of that data, once collected, accompanied by appropriate safeguards? Then and only then do you move to access, which is almost the final question. As we know, the proposals for access in the Bill are actually based on existing law—the Regulation of Investigatory Powers Act or RIPA. That is the last of my concerns that I would like to raise in opening. Justice has massive concerns about the lack of safeguards in the existing RIPA provisions. We think that building these potentially vast—we do not know, looking at Clause 1—proposals on to the existing RIPA framework is simply inappropriate.

Q223 The Chairman: Do you think RIPA has turned out the way you expected when you looked at it in the year 2000?

Angela Patrick: I think there was massive aspiration for what RIPA could achieve, but as it passed through Parliament, Justice campaigned quite vigorously to point out exactly how much of a mess RIPA was going to turn out to be. It is incredibly complex. Actually, the safeguards that are on the face of the Bill are relatively minimal. What you have is an administrative authorisation procedure, backed up by commissioner upon commissioner upon commissioner, which Justice has done a significant amount of work on. It shows that the degree of scrutiny after the decisions have been taken to access data is pretty minimal. Our concern is that, although the aspiration was to make RIPA, post-HRA 1998 compliance, a shining example of a human-rights-compliant framework for surveillance, it simply is not up to the job.

Q224 Mr Brown: Could you both say something to us, in general terms, about the sorts of safeguards you would like to see?

Rachel Robinson: In terms of our approach to this Bill, before we get to the point of considering potential safeguards, we are incredibly concerned about the path along which we are treading. It is only relatively recently that we took a significant step back in 2009, in requiring communication service providers to retain records for minimum periods, records they already retained for business purposes. Now, we are already seeing the next step and we are very concerned about where this path is leading us.

To be quite frank, there is no safeguard that can allay our concerns about the kind of collection provisions set out in Part 1 of this Bill. As I said in my introduction, communications data and its use in law enforcement is a recent boon for law enforcement agencies. It is unique among other forms of surveillance provided for in RIPA in terms of its historic availability to law enforcement agencies. We simply do not accept the premise, the philosophical point, that the state has the right to keep this information about people in relation to whom they have no suspicion of criminal wrongdoing.
Q225  Mr Brown: What about where they do have suspicion of wrongdoing?  
Rachel Robinson: We have never objected to even particularly intrusive forms of surveillance, such as bugging or covert human intelligence sources, where they are based on individuated suspicion and with appropriate safeguards. In terms of safeguards around access, we have consistently expressed concern around the access provisions set out in RIPA, which are mirrored in this Bill. We have consistently expressed concern about internal authorisation processes, the breadth of the permitted purposes for which this information can be accessed, and the range of public authorities that have access. These concerns are, of course, thrown into really sharp focus by the increase and the real difference in the nature of the data that would be retained under these provisions.

Q226  Mr Brown: Is that the same for Justice and is there anything you would like to add?  
Angela Patrick: Justice did look very closely at the RIPA provisions. Before I outline our position on that, we are concerned that Clause 1 of the Bill is a game-changer. It could be, because we just do not know. People are very concerned and quite rightly because, as I say, if you are going to keep information about someone, it has traditionally been done for a purpose. It is almost beginner’s lessons in the common law: we do not do things unless there is a reason to do it. The big question here is whether accessing every piece of information about anyone’s use of the internet, in particular, is justified. We would say it is the starting point for this Committee’s deliberations and must be.  
Moving on to RIPA, we have had exactly the same problems with the RIPA framework in terms of its breadth of gateway, particularly for access through non-law enforcement agencies but also in terms of the mess and the jumble of authorisation mechanisms that exist in RIPA, in terms of different types of surveillance and the different types of authorities that have access to different powers for different purposes. The severe lack of judicial or other oversight of how those powers are used in practice is a point of real concern for us. Administrative authorisation is the norm for communications data access, and will continue to be so, except in connection with local authority use. That is a major point of concern for us, and we just do not understand how you could expand access to communications data without redressing that balance, even if there is evidence for further expansion.

Q227  The Chairman: Thank you very much. I think that is going to lead nicely into what Mr Ellis wants to ask you about. Before that, I neglected to ask each of you to say who you are and where you are in your organisation, just for the record. Ms Patrick first.  
Angela Patrick: My name is Angela Patrick. I am Director of Human Rights Policy at Justice.  
Rachel Robinson: Rachel Robinson, Policy Officer at Liberty.

Q228  The Chairman: We will ask you as well, Mr Killock, to just do that bit at the moment, and then we will ask you to be silent for a few more minutes.  
Jim Killock: Jim Killock from the Open Rights Group, Executive Director.  
Nick Pickles: Nick Pickles, Director of Big Brother Watch.

Q229  Michael Ellis: Going back to the issues that you both were speaking about in terms of authorisation, you say that there is no purpose that you can detect in this, but no doubt you will accept the police or the security establishment would say that there is a purpose, and the
purpose is to help them detect offenders for the prevention of crime and to assist them in their work to keep the country safe. That would be the purpose that they perceive. I do not think it would be accurate to say there is no purpose to the Bill, would it? One would hope that there would be some counter-proposal to that suggestion.

If I can ask you both about your views on the authorisation system, the draft Bill has been criticised by you and others for not requiring public authorities, other than the local authorities—councils and the like—to seek any independent authorisation, by which I mean people like magistrates or judges, to obtain communications data. Instead, the mechanism envisaged by the Bill is a senior designated officer within the security organisation in question, so a senior police officer, say of the rank of superintendent or the like. Do you think that independent authorisation should be required outside of the scope of each organisation? If you do think that, how can you maintain those thoughts when we are aware that there are over 550,000 requests per year? Would that not clog up the whole system?

Rachel Robinson: We think independent authorisation should be required. It is not enough to remedy the problems here, but it is very difficult to see how an independent decision can be made by somebody within the law enforcement agency in question. We are not suggesting for a moment that there are routine abuses going on or any sort of purposeful misconduct on a routine level, but what we are suggesting is that there is an organisational culture problem. If you are working within an organisation, your primary concern is going to be with the operational capacity of your organisation. When it comes to conducting the delicate balancing exercising that takes place under Article 8—necessity, proportionality—an independent member of the judiciary with experience of weighing up these problems and, principally and most importantly, with the requisite independence is the only authority in the proper position to take those sorts of decisions.

Q230 Michael Ellis: If there are over 500,000 data requests, would that not be, first of all, extremely expensive and, second of all, simply not feasible because of the sheer number of requests to a traditional authority?

Rachel Robinson: The first thing to say is that the sheer number of access requests, which has remained at the 0.5 million mark for a long time now, is indicative and just reveals the sheer scale of surveillance that is happening here. That is just on the basis of our current arrangements, and that is a real cause for concern.

Q231 Michael Ellis: Can I just challenge you on that? Just to come back on you to give you the chance, we heard evidence from a previous hearing that, although 0.5 million sounds like a lot—it is a large number—there are something like 25 million recorded crimes in the country. Many crimes nowadays require the use of data of this sort to be solved. To put it in context and perspective, would you not say that the figure is not actually as high as it might be?

Rachel Robinson: There are always steps we can take to reduce crime and produce law enforcement gains. These steps could be things like imposing a curfew on all males aged between X and Y for a certain period. There are always things that we can do that have law enforcement aims, but they are not the kinds of things that we would find acceptable in a liberal society.

Angela Patrick: Can I take a step back? Before you asked your question, you actually made a separate point, which was that you have already heard evidence from Home Office officials,
law enforcement agencies and others about why they think these proposals are needed. I would like to clarify and I started at this point: of course some surveillance is necessary. Some surveillance is crucial and justified, but I would like to remind the Committee that under RIPA there are already very wide powers to access information. This is not about starting from scratch and saying, “Let’s open up key gateways to ensure that we are helping the police solve crimes effectively.” What we are really talking about is whether the proposal in Clause 1, which is to create new mechanisms for collecting and retaining new information, about everybody potentially and anybody potentially—we just do not know—just in case, in order to expand the pool of information that may be needed for criminal investigation purposes and may expand the pool of information that is available for those purposes, is appropriate and justified. That is the real question here, not whether it is appropriate for the police to have access to surveillance powers for the purposes of crime prevention. Of course it is. The question is: what should the powers of data collection and retention look like in order to enable the police to use those powers at a point that is most justified? The question is: how do you approach the balance between infringing the rights of those who might never be suspected of crime, by collecting data about them and retaining it, and on the other side reaching the optimum and most effective mechanism for crime prevention? There has to be a balance there.

Q232 Michael Ellis: I appreciate what you are saying. Can I bring you back to the authorisation point and whether you feel that there should be independent authorisation outside of the organisations and how you marry that up with the issue of the quantity of requests?

Angela Patrick: I am happy to do it. Justice reported last year, having looked at the whole of the RIPA mechanisms, that prior judicial authorisation, in most circumstances, should be your starting point. In terms of communications data, we again said an independent judicial authorisation should, in most cases, be the default. However, we did also say that we recognised, as was explained by ACPO and the Home Office when they gave you evidence, that there are clearly going to be some circumstances where there is an emergency—where there is a pressing time-sensitive issue that requires action to happen now. We accept that, in real terms, those circumstances might arise. We said that, in those circumstances, if you have a law enforcement agency, the police or others, we can see the benefits of having administrative authorisation that is subject to retrospective judicial scrutiny within a reasonable timeframe. We have said two days or thereabouts would be reasonable.

Q233 Michael Ellis: You would agree that there might be permitted purposes for which you would not seek independent authorisation, and particular types of data, so for example subscriber data—just the raw fact of who is subscribing to the use of an instrument. That is not such sensitive information as other types of information.

Angela Patrick: We have said that there is a sliding scale. At one end of communications data you are looking at subscriber data, which is your name, your address, and how you are attached to your account, and, at the other end, user data and traffic data, which becomes, we would like to reassert, much more intrusive. We have in our report said, in terms of subscriber data, if you were simply looking at administrative approval, subject to other safeguards, that
could perhaps be justified. In terms of these other forms of communications data—user data and traffic data—we think that the default should always be, except in that very narrow band of circumstances where there is an emergency, judicial independent authorisation.

Q234 Michael Ellis: Do either of you have any evidence about any individuals who have suffered harm as a result of their communications records being accessed by an investigator? Rachel Robinson: The first thing to do is probably talk about the latest Interception of Communications Commissioner report. Hundreds of errors are identified, even on the basis of the small sample here accessed on the basis of retrospective scrutiny. Two people were detained and accused of crimes on the basis of inappropriate use of their communications data.

Q235 Michael Ellis: Two people out of how many points of data access—hundreds of thousands?

Rachel Robinson: We need to not lose sight of the fact that this came from provisions that were designed, or allegedly designed, to keep us safe from harm. We are seeing repercussions like this but, before we even get to that point—before we even get to errors, abuses or mistakes, in terms of processing or accessing data—we need to look at the very real harm that comes from the retention of the communications data of potentially everybody resident in this country at the moment. We need to think about where we are heading as a society and what is going to be the next step when we build an infrastructure that has certain capacities. What is the next step along that line?

Q236 Michael Ellis: There is not going to be a database as such for this information. The plan is to ask the service providers to retain the data for a period of time, which is not quite the same as a government database. It is not at all the same as that, is it?

Rachel Robinson: We would query the conceptual distinction between that and several smaller databases linked together by government-run processing.

Q237 Michael Ellis: I appreciate that you would query that, but would it not be the case, a possibility at least, that companies could, and in other jurisdictions may well, keep data for their own purposes, without the safeguards that this Bill might envisage. There may not be a time limit, for example, as to how long they would keep data and things of that sort.

Rachel Robinson: Obviously there should be protections around data retention in other contexts also. I think we really do have to recognise the step change here, from a position where companies keep information for their own commercial purposes to a situation where we are effectively contracting out responsibility for keeping records on the entire population for future law enforcement purposes.

Q238 Michael Ellis: Finally from me, is there anything about this Bill that you feel would be non-compliant with the provisions of the Human Rights Act? I think you said, Ms Patrick, that you were the Human Rights Director for Justice. Is that right?

Angela Patrick: I am. Can I simply come back to your last question before I answer this one? Is that okay? I know we are short on time. I agree with Rachel’s position that there are wider implications, not simply of individual cases, about potentially creating a vast storage of data. I
will not repeat what Rachel has said, but I will take you back to my first point. Surveillance is particularly special and states, in the case law around human rights, have been put under a particular obligation because these types of powers take place in circumstances where they are, by their very nature, covert. People who may be subject to surveillance may never know. If you are never prosecuted, if you are innocent but somebody has had to have a look around in your files or used these particular powers, rightly or wrongly, you may never know.

In fact, there is almost a higher burden on the state to look at the safeguards to make sure that they are clearly defined, strict and designed to ensure that only those powers that are necessary exist. Otherwise, the individual themselves may or may not be in a position to seek redress, as they might be in terms of false imprisonment or something else where it is pretty obvious that your rights may have been infringed. They might never know.

Actually, on the question about harm, as Rachel comes back to it, we have often only found out about an error when somebody has let slip that something has gone wrong and that you have been subject to surveillance. Therefore, you have been able to seek some form of redress. That is a very simplistic answer to your question, “Has anyone ever been harmed?” Even if we do have figures or evidence of error or not so much misconduct but mistakes having been made, there is a bigger question and a much more baseline starting point for the Committee’s consideration.

Moving to your second question about human rights compliance, I am again going to say it is a sliding scale. We have looked at RIPA like this. The wider the gateway you make, the more likely it is that, without some form of judicial oversight, in an individual case, if there is evidence that something has gone wrong, there will have been a violation. Now, that analysis becomes much more problematic because there is so little case law on surveillance, because of the simple fact that these cases do not come to light very often. They will often only come to light when there has been a problem, and Liberty will be very familiar with this, having recently represented a lady from Poole who only found out that she had been trailed by her local authority because another local authority employee let it slip.

Actually, the problem we see, looking at the case law, is the courts have been quite robust about the fact that the best safeguard you can put in place is judicial authorisation prior to a surveillance having taken place. They have stopped short of saying you have to have this in all cases.

There are surveillance circumstances where they have said that you do not need a judge but, in most of those cases, it has been the case that they have looked at the facts and said, “Actually, all the other alternatives have been explored; it was a proportionate decision; there were numerous other safeguards in place to offset the fact that you did not have prior judicial authorisation, including the provision for robust retrospective scrutiny.” We say that the provisions in RIPA, which are being replicated in this Bill, fall far, far short of those kinds of robust safeguards. I would be quite happy to take you through why we think the detail of the IPT and the Interception of Communications Commissioner structures are failing, but I know we are short on time.

**Rachel Robinson:** In relation to that specific second question, we think that the data collection provisions of this Bill are not and will not be—are very unlikely to be, in any event—compatible with Article 8. In fact, we think that the provision that exists at the moment is highly dubious on Article 8 grounds. That is before we even get to the RIPA parts of the Bill.
Q239 Lord Strasburger: Chair, could we ask Ms Patrick to write to us with her views on that?

Angela Patrick: Yes, I will do that.

The Chairman: Yes, we are happy to have a paper on your view on the failings of the Interception of Communications Commissioner, how you think it should be toughened up and what teeth it should have. Before I ask Lord Armstrong to come in, you mentioned in your comments that you saw a sliding scale of intrusiveness. I would really like, and I think the Committee would like, to get a paper from Justice setting out what your idea of the sliding scale is, from, I presume, at one end a name and telephone number of the person through the middle-ranking bits—bank account, the tracking of information of where they have been every five minutes.

Angela Patrick: We have actually produced a very hefty piece of research on it, and I am quite happy to have copies sent to all of the Members, if you would like them.

The Chairman: Excellent. We would certainly like that, yes, please.

Q240 Lord Armstrong of Upminster: If one wanted to restrict the scope of this Bill, one could reduce the number of authorities that are entitled to exercise these powers or one could look at the purposes for which it could be made. I want to look at the second of those. There are 11 or 12 purposes in the Bill, taken out of RIPA, which are permitted purposes for the purposes of the Bill. They go well beyond national security, law enforcement and serious crime. Are you happy with that list of purposes or would you like to see it reduced?

Rachel Robinson: We have consistently expressed concern about this list of purposes, which largely mirrors that provided for in RIPA. We feel that it is very difficult to envisage a case that does not involve or fall within the serious crime category in which it would be justified to access communications data. Those other purposes listed, things like the economic interests of the UK, are incredibly broad and encompassing. There is a real potential here to go beyond what is necessary and proportionate and to, in fact, attach to or apply in circumstances that do not involve criminal behaviour in any way. That has always been a real cause for concern under RIPA, under the current arrangements. Of course, now that what we have on the table are proposals that will dramatically increase the amount of communications data and the kind of communications data retained, provisions around access are thrown into sharp focus. They become even more of an issue.

Angela Patrick: I would just go back a step again. Unfortunately, like Rachel I would say the list of purposes does not affect how much data is kept, collected or retained. As a starting point, you keep everything. It does not matter if you are keeping it for the purposes of crime or the purposes of whatever; there is no qualification like that anywhere attached to Clause 1
of the Bill. Basically, it is me, you, the guy you saw on the bus this morning and the person you buy your paper from. Clause 1 enables the collection and the retention of data in connection with yours, mine, his, hers, your mother’s, your daughter’s and everybody’s internet usage. That all gets kept. As to the first two qualifiers that I gave about safeguards in connection with collection, and retention and storage of information, albeit it is not in a government database—it will be stored in private company databases—the question is then: are there safeguards in place to ensure that that information is kept safely and not accessed for other reasons?

The second question I would simply ask is: is that justified, before we get to the question of state access? On state access, we have already said, in order to justify accessing information that is clearly engaging your right to privacy, the state must be able to justify it. We can say that for prevention and detection of crime or for national security etc. I entirely understand it. The further you get away from those core purposes, the more difficult it is going to be to justify. Now, I listened to the Home Office’s and ACPO’s evidence, which was very full. My understanding of the information you were being given from those parties is that they would not like to restrict the purposes, because the real belt and braces was that individuals were being asked to consider, even within those triggers, whether the use was necessary and proportionate. Now, necessary and proportionate are essential from a human rights perspective, but our real concern is, as is stands, there is nobody checking whether that administrative assessment of necessity and proportionality is right. There is no judge who is saying, “Have you got that right? I know that your understanding is that you really need to do this for a criminal investigation. Tick; that has got you in the trigger gateway. What is the necessity and proportionality?” Clearly they walked you through the training that they believe is adequate for that purpose to allow an individual senior officer to apply his mind to that balance but, at the minute, nobody is checking.

The Interception of Communications Commissioner has been reporting on these issues since 2005. Our research showed that, although the very small team of inspectors—there are only five—look through dip sampling each of these different bodies and how they look at communications data, not since 2004 has the commissioner’s report identified any single violation of necessity or proportionality in the decision-making of any public authority. Okay, in his report last week he found one—one out of 500,000 every year since 2004. I am a little bit of a sceptic, but I am also a public lawyer who has acted both for Government and for claimants. In terms of administrative decision-making, no public body expects to get it right 100% of the time. We have said, as Justice, that those figures must suggest that the commissioner either does not see looking at necessity and proportionality as a core part of his role or, alternatively, they simply do not have the expertise or the resources to be able to apply that kind of balance. Of course, applying it retrospectively, in any event, would only get you so far, because the interference has already taken place. We say it is much better to have a prior judicial authorisation in most cases, making exceptions for emergencies, where somebody who is used to applying their mind to those kinds of tricky balancing questions is asked to do it.

Q242 Lord Armstrong of Upminster: Can I just come back to the purposes? To take one extreme case, one of the purposes permitted was where somebody has died and you cannot find out about that. You want to obtain information about their next of kin or about other
persons connected with them, or the reasons for their death. Would you say that the powers of this Act should not be used for that purpose?

Angela Patrick: We would say that possibly you might want to check his pockets first and do other things to check that it was actually necessary to do it. At the end of the day, it may be, if you have no other means of identifying somebody, you might be able to justify that use.

Lord Armstrong of Upminster: Even though there is no crime.

Angela Patrick: If you were targeting the individual who was deceased and you were trying to identify somebody who was connected to him to notify him of his death, you could arguably say that that very narrow purpose could be justified. Again, if you were only opening the doorway to looking at the information connected with a deceased person, you would have to be very careful in terms of the safeguards of how you look at the other information because, clearly, we do not communicate only with ourselves; his communication data will be connected with third parties and other people. If you are only simply using that gateway to identify somebody, they may not object to their data being processed for that purpose. It comes down to the degree to which you are using that trigger and the proportionality and necessity. Have you looked at alternative mechanisms? Do not just jump up and down and say, “Can I use the internet to find out who you are?” A simple check of the pockets or if he has a business card, so you can go and contact his employer, might work better first time.

The Chairman: We appreciate the detail of your answers, but we will need to encourage some brevity, as well.

Q243 Stephen Mosley: A very simple question, and I apologise, Lord Chairman, but I am not a lawyer: is there actually a definition of “necessary and proportionate”? Is it quantifiable or is it measurable at all?

Angela Patrick: Effectively, in human rights terms, what you are looking at is if there is a legitimate aim. In the context of Article 8, there may be other issues but we are looking at what the purpose is for which you are proposing to do this, so prevention of crime, etc. You would look at the severity of the weight for saying that there was a purpose and a reason to do it, and then you would look at whether it was a legitimate aim. Is there any alternative means of achieving this goal? Have you looked at the safeguards to make sure there is no alternative risk?

I am sure Rachel might want to say something else about this as well, but there is a clear set of frameworks that look to show that somebody has actually conducted the balance between the goal at hand and the impact on the individual, in order to look at whether or not they can achieve their purposes through other means. If they cannot, that puts weight on justifying the interference. How serious is the interference at hand—i.e. are we looking at monitoring somebody’s behaviour for months on end? Is it going to impact on his communications for a long time, etc? There are a number of different exercises you go through.

Q244 The Chairman: Could I stop you there? Has Justice got a little paper on proportionality?

Angela Patrick: We can help the Committee with that.

The Chairman: We will happily see a couple-of-page document setting it out, if we may. Dr Huppert, and I will now open the floor to everybody to participate.
Dr Huppert: Thank you, Lord Chairman. Can I just declare an interest, again as a member of the advisory council of the Open Rights Group and as a former member of Liberty’s national council? I got to ask a question in the last session with the two of you, and there was not time for you to answer it. The transcript does not even include the “yes” that you said. One of the assumptions that has been made throughout this Bill is that there is a clear distinction between communications data—the who, the where, the how and so forth—and content. One of the Home Office’s principles is that these are clearly separable. Are you all confident that they are, in fact, completely separate and will always stay that way?

Nick Pickles: For the record, the question I answered yes to was not that question. My answer to this would be no to do an opposite. No, and you will hear technical experts say this but, to use the example of an offshore service provider, if I connect to that service, my ISP knows I have connected to a service—let us call it Yemeni Mail. If they want to know who I have e-mailed within that service, which is the proposal of the Bill, that is content of the communication between my computer and Yemeni Mail. The idea that there is some simple distinction, and that is before you get into encryption and architecture, is disingenuous and misleading.

Jim Killock: Again, I do not think there is. I think the Committee should think of the idea of separating communications and content data, as is proposed particularly in the black box element of this Bill, as applying a sieve. If you imagine you have a sieve, everything has to go through the sieve and then you have to catch some of the communications data in order to establish what that communications data is. This is necessarily a little bit fuzzy. You are expecting and hoping that the algorithms and the computers that you are using are going to do this absolutely cleanly.

Also, often sometimes a communications event may well imply or tell you what the communications content is. For instance, a URL will tell you the whole of the content. If a website is a single URL, a one-page website, then retaining the URL of that will tell you exactly what the content is. Other times, it will tell you merely broadly what the content is. Perhaps if I read the Sunday Telegraph every week that pretty much tells you the content that I am reading. Similarly, if I read the Guardian every week that tells you something different. It either implies about content or, sometimes, it can be the content. In any case, in terms of what the Bill intends to do in terms of retaining communications events, you have to sieve everything in order to find the communication event details.

Rachel Robinson: In addition to the points Jim made there, there is also a conceptual issue here. To what extent does it still make sense to talk about communications data being separable from content because it is less revealing? That is the premise upon which these proposals are based. When we are talking about things like web addresses, how is that less revealing than something traditionally recognised to be content? That is incredibly revealing information.

Angela Patrick: Let me just reiterate that. The traditional description of communications data is “envelope data”, which can be misleading. Actually, in terms of modern electronic communications, there is an awful lot that can be found out in terms of disclosure of the simple information that surrounds a particular communications event—where you are, where the person that you were speaking to was, how long you were speaking to them for, how much data you might have sent them, if you send people their photographs and various other things, and again web addresses. Even the Information Commissioner expressed his concern that you
can learn a lot about somebody from their web history. It is something that you would have to be wary of, but Justice would defer to others on the actual technology. The problem is, with Clause 1 being quite so broad, we do not even have the Government’s explanation of how the technology will work. We have to be slightly cautious in terms of our being able to assist you.

**Q246 Dr Huppert:** Do any of you have any faith in the assurances that are in the Bill and the Home Office commentary that this will not allow for any access of content?

**Nick Pickles:** I assume the Home Office had not read the Bill with regards to postcards, because the last time I received a postcard the content was written on the outside of it. The Bill expressly covers material and data written on the outside of items transmitted in the post, and that is content. There are various other situations where the Bill is drafted in a way where data relating to content could be caught. The basic premise is there.

**Q247 Lord Armstrong of Ilminster:** When I was young, you used to think that what you wrote on a postcard was fair game.

**Nick Pickles:** I would agree with that, but I would also say that it is still the content of a message. If we are trying to distinguish the content and the communications data in that example, the Bill would apply to both.

**Jim Killock:** A postcard being fair game for your relatives is a different thing from a postcard being fair game for the security services and for private companies to log on behalf of the Government for future investigations.

**Lord Armstrong of Ilminster:** If I sent a postcard that had sensitive security information on it, I think I should be fully entitled to be found out.

**Q248 Dr Huppert:** Do you want to just comment on whether you have faith in the assurances? You do not have to comment on every question.

**Angela Patrick:** I was just going to add a very brief point, which is that, although we have problems trying to assess how much faith we should have, because we do not know what the technology is that is going to be used and we have not had the Government’s explanations, even on the existing rules in RIPA, look at the Interception Commissioner’s report, albeit that he only identifies a few mistakes. Mistakes there are, not least local authorities completely misunderstanding the type of data that they are allowed to ask for. Local authorities are expressly barred, on the face of the statute, from seeking data for purposes other than the prevention and detection of crime, but are expressly authorising themselves to get that data until, just by chance, the Interception of Communications Commissioner may have audited it and said, “Actually, you have asked for it and it is ultra vires. You should never have asked for it.” Mistakes happen.

**Q249 Dr Huppert:** Can I return briefly to the way that communications data works? It is split in the Bill into traffic data, use data and subscriber data. Subscriber data we have discussed as being roughly equivalent to a telephone look-up. Actually looking at the Bill, it says it is information other than traffic data or use data held or obtained by a person providing a service about those to whom the service is provided. Would your reading of the Bill therefore mean that, if it was my Facebook account, that would include any posts I had
made, any pictures I had put up or any likes I had made? Would that count as information held about somebody to whom the service is provided or would that count as content?

Jim Killock: It is subscriber details. A lot of this is subscriber details, because your profile on a service is all the set fields that you have to fill in, in order to create or maintain an account. On Facebook that would certainly include your date of birth, marital status, sex and age and so on, but also, as you say, the likes that you had made, the particular interests that you had identified—quite a considerable amount of information that would really be content, except that it has been attached to your profile and is, therefore, in the terms of the Act, subscriber details. There is an obvious case to just slim that down to a number of set details that may be described as subscriber data.

Q250 Dr Huppert: That is very helpful. I will just ask one last question, and then move on and let somebody else ask questions, which is about the effect internationally of this. It would be interesting to get some sort of perspective. I know some of you have addressed this in your previous comments. Joe Biden, the Vice President of the United States, said that, where countries pursue monitoring arrangements, that could lead to businesses moving abroad to avoid those arrangements. Are there other countries that have techniques like this, which use black boxes like as proposed? Do we think there would be harms locally to our industry for having that?

Rachel Robinson: Our understanding is that the only countries that use this kind of DPI technology on a national level are, in fact, China, Iran and Kazakhstan. I know this was the evidence given to the Committee last week. We have not undertaken detailed comparative research but, on the basis of what we have established so far, we understand that is the case. We also understand, in a number of other countries—Egypt, Pakistan and Tunisia—DPI software is used at a local level for monitoring and surveillance of the population.

I think we have to be very concerned about our position here. With countries in Europe, as I said in my introduction, challenging the constitutionality of current arrangements, and given that this Government committed to ending the retention of data unnecessarily, we have to think about the direction that these proposals are taking us in, and also bear in mind that the current arrangements are subject to challenge—reference has been made to the European Court of Justice. It is something to bear in mind.

Q251 The Chairman: Which other countries across Europe are challenging them?

Rachel Robinson: Our understanding is that Germany has found the provisions to be unconstitutional, the Czech Republic, Bulgaria—and I am afraid the other two escape my mind, at the moment.

Jim Killock: Romania and Cyprus.

Nick Pickles: Ireland is challenging the existing the data retention directive in the European Court of Justice.

Q252 Stephen Mosley: I am very interested in Clauses 14 to 16, which establish this filter. It has been described as a filter by the Home Office people whom we have spoken to. You can probably look at it the other way around; other people might describe it as a search engine to go out there, pool all this data together and send the results out. What are your personal views on this and do you think the filter protects or impinges on an individual’s privacy?
Nick Pickles: To refer to the earlier point, the filters highlight this change. Rather than having small amounts of data held that we pursue with a named individual or a named device, the filters are the way of bringing lots of data together to produce a result like a search engine would do, without necessarily requiring that data. One technique currently used is geoboxing. You say, “Here is a box on a map. Tell me every device, from this data, that has been within this area.” The filters are intentionally the enabling part of the database function. Whether it is a central database or lots of little databases is irrelevant; the output to the officer is the same. Those filtering provisions are so broadly worded and so poorly drafted that they could allow mining of all the data collected, without any requirement for personal information, which is the very definition of a fishing trip. The metaphor someone else used is this will be fishing in the sea with a net made of string. We will catch some small fish but the sharks will still carry on.

Rachel Robinson: I absolutely agree with the points made there, and I would just add that we are incredibly concerned about the role that these filtering arrangements provide for the state at the very centre of these proposals. These filtering arrangements will essentially join up the system of databases to create an integrated system. They will take the atomised pieces of communications data and form them into an incredibly revealing, incredibly full and detailed whole. In some circumstances, this will be done in order to establish the validity of the requests in the first place, before you have even established that the request is a valid one. That is a real concern for us.

Jim Killock: This area does create a very large number of potential risks, because you can remove people’s privacy through several steps if you can match up data. You can attach a number of different identities to one person, for instance their mobile phone, their normal phone, their work e-mail, their personal e-mail, their Facebook account and so on. Then you can build up from that a map of all of their communications, both in time and, to a certain degree, in space as well because you have the geolocation data. Because you can do that mapping not only against one person but other people, you can potentially identify people like whistleblowers. You can identify journalistic sources, and perhaps people who are worried about their legal position and are trying to consult somebody for legal advice. In all of those sorts of cases, where somebody might be either technically or actually breaking the law but, nevertheless, is acting in the public interest, they are going to be extremely dissuaded from taking action. That can have severe impacts, not just for exposing potential corruption within government, the police or elsewhere; it can also damage journalists’ relations and their ability to report, and client/lawyer relationships. That is one set of potential risks that come from connecting this data up. I know that the Home Office is saying they are not going to use this data in this sort of way, but that is pure intention. The data will allow you to do this. I cannot imagine how they are going to be able to justify to themselves not using capabilities they have spent several billion pounds on.

The other set of risks comes from the ability to hack, which partly comes from the fact that you have got a distributed database and there are multiple access points, and these access points are available across the internet. You might think that I am sitting here saying, “What do you mean ‘hacking’? This surely is not going to happen. We are going to be able to keep this data very secure,” but I think we outlined in one example last week a little bit about what happened with Vodafone in Greece, in 2004, when the data of the Greek Cabinet, senior police officers and so on got accessed through a government back door that had been installed.
in the equipment that Vodafone had. It was hacked by persons unknown, and they got fined something like €70 million because of this data breach. The data breach occurred because the Government had asked their equipment provider, Ericsson, I think, to install back doors that they might want to use in the future. The back doors were not enabled because Vodafone or the Greek Government did not pay for the back doors to be enabled, but they were there and so somebody used them and we still do not know who. Suspicion lies with the US Government, but that is not a given.

The other example, which was in 2010, I think, was that Google had been asked to provide government back doors so that people could make surveillance requests similar to the sorts of things that are being proposed here. A number of people were attacked from China. Somebody from China, presumably the Chinese Government but I do not think anyone has conclusive proof, gained access to that data and obtained some of the e-mail records of Chinese citizens. I think it is believed that that was done for political reasons. Again, this was a government-mandated back door installed; it was meant to be secure, and was accessed by people who have criminal or political intent, from a foreign jurisdiction, which you have very little control over. This is a real risk that has been created. When we talk about where the proportionality and necessity is for collecting data, we have to recognise that, in collecting data and creating access powers, we are creating genuine real risks to every citizen, if we are collecting data about every citizen. That is why, traditionally, surveillance is targeted at individuals. That becomes much more important in this data-rich world.

Q253 Stephen Mosley: You have highlighted some problems with back doors. Surely the advantage with this Bill if you legislate for it, if you put this filter in place, is that within the filter you can have security, you can have audit, you can have logging and all these things in the filter, so there is no need for back doors. Surely we should be trying to make sure that this Bill legislates for it all and provides the framework so that it can all be done legally, above board, without the need for back doors.

Jim Killock: How does a filter work without accessing a number of databases and comparing that data? Without a single database, how do you do that without there being a number of databases, all of which have access?

Q254 Stephen Mosley: There is one other area within Clauses 14 to 16 that concerns me. It does not actually specify who will own, run or look after this filter. In fact, it gives explicit power to the Secretary of State to transfer the functions to other designated public authorities. Have you any thoughts on that?

Rachel Robinson: We have concerns about that. There is the obvious uncertainty, which is a problem in and of itself, but there is the potential that this creates for filtering arrangements to be run by, for example, an organisation more on the front line even than the Home Office. That has to be a real problem in terms of operational involvement and the ability to impartially operate a service so central to the system. That is one concern. In terms of co-opting other authorities, the Information Commissioner, etc., into the system, they are effectively and should be a check on the system. Co-opting them into the system in that way would not, we feel, be appropriate.

Nick Pickles: Far be it for us to cast aspersions on the Home Office’s ability to manage things they have contracted out.
Michael Ellis: I would not have thought that was appropriate. It was a contract with LOCOG, rather than with the Government was it not?
The Chairman: Let us move on.

Nick Pickles: I accept the clarification. I think the point is absolutely right that where you allow these filters to sit is central to the way that the information will be accessed and how the filters can be used. I return to my earlier point: who is stopping these filters being used for unnamed searches—for situations where certain profile criteria may exist? The purpose of the filtering is to show me who meets these criteria, rather than show me what this individual or device has done. That is the role of the filters. If that is anywhere near the front line, you have a serious risk of conflict of interest and of abuse.

Q255 The Chairman: Mr Killock, you said, without getting into conspiracy theories here, that it may have been the United States Government that leaned on Google to build in back doors to the Greek system. In view of the fact that Google and Facebook are giant American corporations and they have to keep the American Government happy, and the British Government is hoping that Google and Facebook are going to co-operate to give us, the British Government, the information we want, how concerned are you that our friends in Homeland Security may lean on Google and Facebook to give them the information as well?

Jim Killock: Certainly that is a considerable worry, and there is a lot of co-operation there. We have to be a little bit careful here. This discussion is actually about police access. Other sorts of access are not especially in the scope in this conversation. I am not saying they are not of interest to you—they should be of interest to you—but in terms of trying to understand quite what the dynamics are, I think we should be a little bit careful to say this is about police investigations, Special Branch and other parts of law enforcement, rather than the sort of surveillance and access that MI5 in this country would have. They have a different regime, which I am sure we would be delighted to discuss, but I think it is probably a little bit broader than the Committee wants to take on, at this point.

Q256 Baroness Cohen of Pimlico: I have two questions, one of which I think you have answered. I think everybody is telling me that communications service providers are not going to be able capture communications data reliably and store it safely. I will just check that there is no dissent there. One of the objections always made by anybody to inquiries, or what they would view as repressive sorts of inquiries, is that criminals, terrorists and bad guys could easily and cheaply avoid the production of communications data. Do you have evidence of this? Is this a point that you guys would make or am I putting words in your mouth?

Nick Pickles: The Home Office accepts that they will still have a capability gap of 15%, even if this project is 100% successful. I would ask any government department to produce a demonstration of an IT project that has been 100% successful. The real nightmare situation is not the data being lost, in reference to the first part. The nightmare situation is someone watching it. If you are not interfering with the data, but you are watching who is communicating with whom, when and where, that information is extremely commercially valuable in terms of espionage, but also in terms of simple stock market manipulation. The nightmare situation is someone watching, not stealing.
Q257 Craig Whittaker: Could I just interrupt there? With all due respect, if people were going to do that, do they not have the capability to do that now anyway? Is that not a bit of a red herring? If somebody is going to do it illegally, they will get on and do it.

Nick Pickles: To use the example of a commercial webmail provider, they have an incentive to keep this data secure, because that is their business model. They will say, “If our security is breached, our product is less attractive.” A CSP does not have that incentive. A commercial service provider does not have the incentive to keep data about your e-mail use secure, because they do not want to hold it in the first place. If that security breach did happen, the CSP’s first response is, “We do not want to hold this data and we are being forced to hold this data by a Bill.” There is a serious question to ask about the motivation.

The attacks referred to previously were aimed at Gmail, and Gmail largely resisted those attacks. Can the same be said of an organisation that does not have a commercial motive to protect that data? Indeed, it could be someone working within that organisation. There is a risk there to that data, a serious risk, so you have the risk of abuse of access, not just loss. On the second point, I will defer to colleagues.

Jim Killock: Sorry, what was the second point?

Q258 Baroness Cohen of Pimlico: The other point I was asking about was the general statement: “You might as well not do all of this, because criminals and terrorists will get away from it anyhow.”

Jim Killock: There are two areas we are thinking about here. One is commercial services, which is the vast majority of internet communications. Then there are personal-to-personal types of communications, which might well avoid some of those commercial services. Most of those communications from one person to another person on the internet are done entirely securely not using commercial providers. Most of that is done by business. Most of that is things like virtual private networks, where businesses want privacy and they do not want their information shared with third parties, so they avoid that.

The amount of communication that is done by citizens in that sort of way, where there is no record kept by a company like Google or Facebook, I am pretty sure is vanishingly small. It may get bigger or it may not, but I think that is something you need to hear from the technologists that you are talking to. My sense of this is that most ordinary communications are conducted through large organisations because that is where the investment is. Google invests lots of money in getting people to use Google, and so does Facebook. People like the services they provide, so they use them. Therefore, records are kept because they have them for business purposes. Therefore, law enforcement can get access to them.

The idea that we are getting a decline really needs to be spelt out by Charles Farr and colleagues at the Home Office. I would just point out that the Home Office’s own paper says, as I mentioned in my opening statement last week, that there is an assumed 1,000% increase in data going across networks. The Home Office accepts that. When they say to you, “We will only have 65% of the data rather than 75% of the data,” what they are saying to you is, “In 10 years, we will have 650% growth if we have nothing, but we want 750% growth.” Their statistics pretty much bear that out. We need to know what exactly that 100% growth they are not getting entails, and why it is that they might find it difficult to access that, given the huge commercial availability of communications networks.
**Rachel Robinson:** In addition to the very sophisticated potential methods that have been mooted here for potentially evading or getting around the proposals set out in the Bill, there are also methods of very little sophistication that could potentially be used to get around these proposals. For example, there is the use of a pay-as-you-go mobile phone with an anonymised SIM, so the possibilities for evasion range from those with very little sophistication to very sophisticated encryption and anonymisation techniques, hijacking the unsecured networks of others, etc. It is a wide ranging problem.

**Jim Killock:** I might add that one of the rather better known techniques for avoiding government surveillance is Tor. Tor is largely paid for by the American security apparatus, or has been, largely because they want to enable Chinese dissidents to avoid surveillance from the Government there. It cuts both ways at all times.

**Q259 Lord Strasburger:** I have some questions about safeguards to prevent misuse of data. I think we may have strayed into these areas already, so we might be able to get through these quite quickly. There are concerns about the potential misuse of communications data. Do you consider that the draft Bill seeks to address these adequately and do you have any evidence of any abuse under the current RIPA safeguards?

**Angela Patrick:** I will start off, because I think I will be very brief, but the others can deal with the technical issues. Our starting point, to repeat what I said earlier, is not necessarily about abuse; it is about the expansion of retention and collection. As we know, when you expand the amount of information you keep, it becomes more difficult to manage. The likelihood that you are going to have mistakes—not misuse necessarily or abuse, which is a potential problem but not necessarily the major one—increases when you expand the potential for error. You have to look in great detail, if you are going to expand, and we do not know how, why or what. We are a bit concerned about what the actual expansion will involve, and we are very concerned that no justification has been provided so far.

When you are looking at that expansion, you have to look at what the safeguards will be and nobody has told us what they will be. Actually, it is incredibly difficult for us, as informed commentators, to try to help the Committee understand the risks, not only of misuse but of error. We have to simply look at the fact that these databases, as much as they will be automated and otherwise running on various programs, may themselves be fallible. They will be designed and run by human beings to a certain degree. We all know that, when it comes to data, people do make mistakes, often very costly ones for those who have simply had their data stored. They may never have known that it had been stored, but now may have the concern that it is either in the ether or sent elsewhere, with no knowing who has it.

**Q260 Lord Strasburger:** With respect, we have heard all that before. If you could concentrate on the safeguards and whether you think they are adequate, that would help us.

**Angela Patrick:** The problem is we do not know what the safeguards will be, because we have not been told what the technology is going to be and we do not know how it is going to be stored, except that there is going to be some agreement between the Government and CSPs. We heard the point made earlier that it is okay because it is not a government database. It is private companies managing data that, as my colleague has said, they have no real commercial incentive to keep. Actually, the question is: do we trust the private sector to keep these databases secure? If we do, what is the detail, where is the trust and what are the safeguards
that are imposing on them obligations to ensure that there are protocols in place not just to avoid misuse but to minimise error?

Q261 Lord Strasburger: Do you have any evidence of misuse under RIPA?
Angela Patrick: The best evidence we have is the Interception of Communications Commissioner’s reports.

Lord Strasburger: Your best evidence is the lack of evidence.
Angela Patrick: There is a lack of evidence, but also look at the mistakes that were self-identified. There are not many of them; I think the figure is 900 across law enforcement agencies. They identify that they are fallible.

Jim Killock: I have one quite interesting piece of evidence. Obviously the public authorities now report most of the time. That is the evidence we get, but one of the complaints that has been made about the current access regime has been that Google does not comply with enough of these requests. I think they have been turning down something like 30% or 40% of the requests made to them. Why have they been declining 30% or 40% of the requests? Because they have been inadequately framed; they have not been signed off by officers. It is not because they think that they are entirely inappropriate and they will not deal with them; they just send them back as poorly formed. If that is the case, Google has given us the only real example of how these requests are statistically performing; we do not really have that as quantity from the Interception Commissioner’s reports, because they just give numbers and do not tell us what the sample size is. If Google is correct in saying they have to return 30% or 40% because they are badly formed, we have some evidence that this is not working very well.

Rachel Robinson: In relation to the first part of this Bill and data collection, in terms of safeguards, all we really have are empty assurances or requirements that data needs to be kept securely, without more. That is a cause for concern. That stops us from scrutinising, potentially, the safeguards envisaged by the Government. In terms of access arrangements and other parts of the Bill, many of the safeguards proposed are process-related—formal requirements, for example, that the requisite individual would be named in a notice, etc. There is very little in the way of substantial safeguards there.

Nick Pickles: The very definition of abuse is sketchy, because the problem is that if, currently, an officer views acquiring data as necessary and proportionate, it is by definition not abuse. As we heard the other day, there are police officers who think it is necessary and proportionate to use this data for road traffic offences. Is that an abuse? No, because the process was followed and the criteria are satisfied. Is that a fit use for a surveillance infrastructure not used in a democratic state anywhere else in the world? I would say that is not a fair use but, by definition, the officer said it was necessary so it cannot be abuse in the legal sense.

Q262 Lord Strasburger: Thank you. Some of you have suggested that the powers in the draft Bill might put off whistleblowers or endanger privileged communications, such as with lawyers. Do you think these are real risks, despite the permitted purposes and the authorisation regime? Are there additional safeguards that could be introduced to lessen these risks?

Nick Pickles: RIPA explicitly fails to recognise privileged communications. The Bar Council and the Law Society have both been very clear that there is no recognition for privileged communications at all in the existing regime. Indeed, there is no recognition for privileged
communications with MPs. I understand the Home Office has still to respond to concerns about the Wilson doctrine with regard to this legislation, which were clearly raised, given that a constituent contacting a Member of Parliament would have their e-mail recorded. There is a clear issue there. I would refer to colleagues on that for further points.

Jim Killock: We are speculating and we need to really understand and see precisely what the filtering arrangements in particular reveal. I would point to Ireland as an example of where this has occurred. The cases being brought by Digital Rights Ireland, I believe, involve individuals whose data was abused. There was a recent article in the Guardian—I will send the details of that to the Committee—where again there have been cases of journalists and police finding data incorrectly used and inducing some degree of a culture of fear among some of those groups. It is entirely possible, once the data is collected, for that sort of thing to arise. We have to firstly understand what the proposals really are. I do not feel those details have been explained to the Committee and us. Then we have to start to understand how the data that is being collected might actually be interrogated. We certainly see, in other countries, some indications of how it can go wrong.

Q263 Craig Whittaker: At one end of the scale, we obviously have the Government, police and security services saying they have a need. At the other end, we have you guys, who I think are saying the Bill is not fit for purpose. What would you suggest we do to make it fit for purpose?

Rachel Robinson: The answer is that we just do not think the case has been made for these types of proposals. When you are embarking on a human rights assessment of these proposals, you have to look at the revealing nature of the information, of course. Then you have to look at potential law enforcement gains. The idea or the suggestion that these proposals will lead seamlessly to gains in law enforcement is something that we would challenge. We are told that, in 95% of serious criminal investigations, communications data plays a role. We are not told, however, how many of those investigations lead to successful prosecutions and what kind of a role communications data played in those prosecutions. Was it central? Was it peripheral? Were there other techniques that could have been used in order to get to the same point?

Q264 Craig Whittaker: In your opinion, then, nothing would make this fit for purpose.

Rachel Robinson: In our opinion, the data retention arrangements that we already have in place are very hard to reconcile with the protection of personal privacy. The blanket retention of data about individuals, as opposed to targeted surveillance, with which we have no problem, should not be a feature of a liberal society.

Craig Whittaker: In your view then, absolutely nothing can change in this Bill to make it fit for purpose.

Rachel Robinson: In our view, the basic provisions set out in this Bill—take away reference to access and scrutiny, which basically replicate current provisions—are to require communication service providers to retain data that they would never keep for their commercial purposes, as essentially an arm of the state for these purposes. We do not think that that can be justified.

Craig Whittaker: No, then there is nothing that can be done to make this Bill fit for purpose.

Rachel Robinson: Yes.
Q265 Craig Whittaker: What about the other witnesses?
Angela Patrick: We are concerned that, basically at Clause 1, we just have not seen the evidence, not least that we do not quite know what the scope of Clause 1 is. If the assumption is that, reading it as drafted, it creates a very large power to, as Ms Robinson said, collect pretty much any information that passes from anybody through a CSP, then that is a big ask. Actually, what you have to do as a Committee, and as an objective observer, is look at what this gets us. What does it gain? We have quite a wide gateway provision in RIPA already. What you are talking about is adjusting the ask to the evidence that it is needed. The problem we have is that we have not seen the evidence from the Home Office, other officials and data users for why this vast expansion is justified.

Q266 Craig Whittaker: What would you do then? What would you suggest?
Angela Patrick: If you were asking me to rewrite the Bill, I would drop the first part and read our report on RIPA. Do not expand the collection and retention of data; just up the existing safeguards in RIPA to perhaps make it fit for purpose in the first place.
The Chairman: That was very clear and concise, thank you.
Jim Killock: The problem we have here is that we do not have a clearly defined problem to give an answer to. What we have is a bald statistical statement that access to communications data is going to grow by 650% rather than 750% or, if you want to phrase it the way the Home Office does, it is going to decline from 75% to 65% access.

Q267 Craig Whittaker: Could I ask you, yes or no? What would you do, if anything, to make it fit for purpose? If you do not think it is fit for purpose, could you make it fit for purpose or do we just kick it out?
Jim Killock: Given that we do not really know the problem, it is an incredibly hard question to answer.
Craig Whittaker: With all due respect, you have a lot to say on this Bill to say that there is very little information in it.
Jim Killock: There are a lot of implications from what the schemes appear to entail—that is to say filtering, databases, connecting databases, extra powers to collect—but there is no indication of what precisely is being targeted and why. It seems to me there are two things going on. Firstly, the Home Office believes that, by connecting data up and being able to make queries against it, they will gain some very nice, extremely intrusive, revealing and important-for-them new powers, which they do not really wish to discuss with the public and tell us that it is about maintaining capability. That is one reason why they are doing it. Secondly, there is some possibility, given that they are saying that there is this gap between what they might access and what they are currently going to access, that they are finding it difficult, in some circumstances, to get hold of communications data that exists. But when we ask what that communications data might be, we get told things like, “We do not really want to discuss that, because that will help people hide themselves.” Without that information, trying to fix this Bill is very difficult. There is probably something in trying to develop better relations with overseas companies, understanding how it is that they get data, whether the legal regimes are sufficient and whether police officers understand how to get that data from overseas companies. There is a bunch of questions like that.
Q268 Craig Whittaker: In your view then, it is not fixable.

Jim Killock: No.

Nick Pickles: The Bill is not fit for purpose and that was the view that I took. It was also the view that the current partisan Government took in 2009, when they opposed the same thing.

Craig Whittaker: What would you do to fix it or would you not fix it at all?

Nick Pickles: It requires the monitoring of every communication made by everybody in this country.

Craig Whittaker: Would you fix it or would you not fix it?

Nick Pickles: It is distinctly undemocratic, so I think it should be thrown out.

Craig Whittaker: You think this should be thrown out. Thank you.

The Chairman: We must be brief if we can. We are running rather late.

Q269 Michael Ellis: Just briefly, in fact there was a difference in the Labour proposals of 2009, was there not, Mr Pickles? That called for a central database whereas this does not. I would just correct that.

Nick Pickles: I would challenge that immediately. If you have a look at the 2009 consultation document issued by the Home Office, it states quite expressly the Government rejects a central database, and the Information Commissioner welcomed that in their response to the 2009 consultation.

Q270 Michael Ellis: As far as what the problem is, the mischief that this Bill is attempting to redress, all of you tended to say that you do not see what the problem is. Is it not obvious, and have you not now heard the accounts of others, that technology has moved on? Communications data has moved on. The authorities are saying they can no longer monitor in the same way that they used to be able to, when it was landlines and mobile telephones. There has been a degradation in their monitoring ability. They want to stop terrorists and criminals from committing offences. That is obviously the case of what they are trying to achieve, is it not?

Jim Killock: It needs to be really spelt out exactly what that means.

Michael Ellis: Hold on, Mr Killock. You have said that, but you also seem to want the authorities to tell you and your colleagues what it is that criminals do to avoid detection, so that anyone listening to this Committee who has bad faith in mind can use those tactics to avoid criminal detection.

Jim Killock: Under current data retention, we know exactly who retains data and what. We know precisely which ISPs are retaining logs and exactly what are in those logs. When it comes to the inaccessibility of data, we need a bit more than assertions. An assertion that goes around Parliament a lot is, “What about Skype?” That is quite an interesting one. Skype is peer-to-peer, so calls go from individual to individual. Presumably they do not produce data trails, but Skype is also an application owned by Microsoft. There are some centralised parts of their network and there are back doors built into it. I am afraid that, in order to understand what this apparent capabilities gap is, we are going to have to hear what types of communications are not being accessed in what circumstances.

Angela Patrick: I just want to add that we started our research that we did—and I will provide that to the Committee—on the basis that we thought there were problems with RIPA. Part of
it was that technology had moved on. That is where we were in the 1970s; we were saying, “Gosh, technology is racing ahead and the privacy laws are not keeping up.” The question is: technology is racing ahead but that also means that what you could be looking at are vastly greater powers to monitor individual activity by capturing data. For example, we used a very facetious example at the start—envelope data. It does come from “Let’s track who sent what letter to whom,” or how the telephone exchange knows who is speaking to somebody else. That is a very limited amount of information—who called whom when, who wrote to whom when, what their social communications are, how often they speak, etc., but technology has advanced in such a way, as we have explained, that we can tell where you were, how much information you sent to each other, how often you met and what your history on the internet was. It is a changing pattern, and we would not like advancing technology to be used to mean that we are depreciating the amount of data we can collect. It is simply that advancing technology is perhaps opening up avenues for surveillance. The question for parliamentarians must be: what avenues are appropriate, proportionate and necessary?

Q271 David Wright: Can I just turn briefly to the monetary costs and benefits of these proposals? You may have seen the previous evidence that we have taken, where Home Office officials have given us estimates of the net cost of the draft Bill. They are saying it will be £1.8 billion over the next 10 years. Do you think that is realistic? Secondly, what do you think about the net benefits figure that they have calculated of £4.4 billion? Again, do you think that is a realistic figure?

Nick Pickles: I might note firstly that I formerly worked for an IT contractor, at the time when the Public Administration Select Committee was producing its report into the rip-off culture in IT. I would urge the Committee to read that report if they are interested in how IT contracts are procured. The Minister could not even bring himself to say at the Dispatch Box that the £1.8 billion estimate was accurate. The Parliamentary Question from Duncan Hames MP asked about that; the Minister could not say so. We have also asked the Home Office to provide details of the breakdown, so both the cost and the benefits, and where they fall. We have been told we cannot have this because it affects commercial interests, security and law enforcement, which is surprising given that the majority of the benefit falls on HMRC. I cannot quite see how tax returns are either commercially sensitive or, indeed, security or law enforcement. I would merely refer to the Government’s own IT strategy, which says there is a presumption against IT projects over £100 million, because they do not work.

I would refer to the fact of whether there is a competitive market. No, because, as we have heard, suppliers do not know what they are supplying. Is Government an informed buyer in this situation? Again, I would refer to previous IT projects. Will this software be non-proprietary, so available and integrated? No, because, as we have previously heard, suppliers will only be told in certain instances what they are building. Finally, will it integrate with the existing legacy estate? As the Public Administration Select Committee looked at, the Government has no interest in understanding this because it will cost too much. In answer to the £1.8 billion of costs, I will eat any hat if it costs £1.8 billion, because it is simply not true; it will not happen and the idea that this will come in on budget is simply remarkable.

Q272 David Wright: Your view is it will be a lot more than that.

Nick Pickles: I think it will be a lot more by a factor of 10 at a minimum.
David Wright: How much risk will the private sector bear?

Nick Pickles: From past experience of government IT projects, very little. From every IT contract ever produced, and indeed if you look at the National Audit Office reports today into the Home Office’s management of the Border Agency, weak leadership and poor project management remain a hallmark of public sector procurement. I see no signs of that changing anytime soon. This would make history as the first government IT project to come in on budget, on time.

David Wright: What you are saying to the Committee is that you estimate 10 times the cost that they are quoting.

Nick Pickles: When the first proposal was floated in 2009, estimates were actually £18 billion.

Q273 David Wright: Anybody else?

Jim Killock: I do not know that I can say exactly what the costs will be. You need to hear a lot more again from the Home Office. We need those breakdowns to understand precisely what the proposal entails and where the potential cost overruns might be, but the fact that Charles Farr, who proposed the interception modernisation programme under Labour, sat here and told us that black boxes were not a particularly big concern for this Bill tells us that he has put his ambitions, and the Home Office have put their ambitions, for large-scale data collection through black boxes on the backburner. Now, that may well be because money is a little bit tight right now. It may well be, especially given the fact that the Bill is an enabling Act that allows new collection duties to be imposed over time, either directly on service providers or through these collection procedures and black boxes—either route—that you could easily see new categories of information being included, new duties of retention being included and the Bill going up, purely because people say, “Here is another thing we want. Here is another thing we want.” Over time, you end up with a scheme that looks remarkably similar to Labour’s original proposals and the costs look remarkably similar, even though the promise originally was rather less ambitious. I think it is promising a lot to say that this is going to stay.

Rachel Robinson: The only thing that I would add to that very comprehensive answer is that, as technology develops, there is a great deal of technological opinion to the effect that the costs of adapting infrastructure to deal with new technological developments will be great, endless and constant. That is a real concern.

Q274 David Wright: What about the cost of the additional regulatory regime that was being proposed earlier? One of the things you were suggesting—I am changing tack a little here—is that you wanted greater oversight, for example through the judicial process. Have you got any estimates of any additional costs that would be incurred, if we had further judicial oversight, in terms of giving permission to search for data?

Angela Patrick: We have not extrapolated that. There is some data in connection to the extension of judicial oversight to local authority decisions under RIPA. I am sure that, if you wanted to ask for that information, the Home Office could compile it by extrapolating the costs that have been incurred by local authorities asking magistrates, as opposed to going through the traditional administrative route.

Jim Killock: One cheap point for the proposals that some of us have raised is the idea of notification. As you are hearing from the police and so on, there are going to be times when notification should not occur; somebody who has been investigated should not be notified
because they are going to be under continuing investigation or are suspected in that sort of sense. Simply telling people that they have been investigated and their data has been supplied is not going to cost very much at all. That could provide a lot of evidence about abuses, if particular populations are being profiled, if particular individuals are being somewhat hounded or if the investigations were just simply inappropriate. That might be a very cheap means of proving transparency, if you like.

**The Chairman:** We need to move on, Mr Killock. It is an area of interest we wish to explore, but not right today. Anything else, Mr Wright?

**David Wright:** That is it. Thanks, Chair.

**The Chairman:** Thank you very much. I am sorry we have overrun horribly, but thank you all very much. We could have gone on much longer interrogating all of you and getting the excellent information from you, which we will chew over. Please send us, those of you whom we have demanded them from, the papers we have asked for. Thank you all very much for giving your evidence today. Could I ask you to move quite quickly, so we can get the next evidence people in? Sorry for being so rude, asking you to move quickly.
Professor Anthony Glees and Dr Julian Richards (QQ 275-329)

Examination of Witnesses

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

Q275 The Chairman: Welcome, gentlemen. Sorry for keeping you waiting but, in nearly all our evidence sessions we seem to run a bit late. We find them fascinating and we interrogate at length. For the record, could you state who you are and your position?

Dr Richards: I am Dr Julian Richards. I am the Co-Director of the Centre for Security and Intelligence Studies at the University of Buckingham.

Professor Glees: I am Professor Anthony Glees, and I am Director of the Centre for Security and Intelligence Studies at the University of Buckingham.

Q276 Lord Strasburger: Professor Glees, you stated on the “Today” programme in April that one of the arguments for the proposals in the draft Bill is that it needs to be done because it can be done. Why does the ability to access communications data necessarily mean that public authorities should be able to access it?

Professor Glees: In a radio interview it is not easy to get an extended argument across. What I meant by that was this: if there is unregulated space, and there is, and if this unregulated space is used for criminal purposes, and it is being so used, and if it possible to mine such space to make it regulated and to apprehend criminals, then it should be done. That is a very straightforward issue; it is not 50 shades of grey. It is a black and white issue for me.

Q277 Lord Strasburger: What limits do you think need to be applied to state intrusion into people’s private data? Are there, in your mind, no limits?

Professor Glees: There are limits, but what those limits are is a rather deep philosophical question. The other way of looking at this is to look at the sorts of regulations that exist—for example, the Acquisition and Disclosure of Communications Data Code of Practice in its 2007 version, which I have read with interest and care. That seems to me to be an excellent way of ensuring that the correct boundaries are kept. As I say, there is a philosophical point here, where you have people putting all sorts of intimate details about themselves quite freely on to the internet. What is private and what is public no longer means what it meant when I was a student 40 years ago. One does have to have that debate. As I say, in my view the correct way to look at it is to ask yourselves what the codes of conduct are—the ways in which practice is regulated. I think, in the documents that I have seen, it is extremely well regulated and that people should not be afraid of this.

As I say, at the end of the day, what this is about for me is the introduction of some kind of lawfulness into cyberspace. It is self-evident that something that is already being done should be done in areas where it can be done and needs to be done. That there is this public disquiet about this so-called “snoopers’ charter” seems to me to be not an issue that has anything to do with the facts before people, but is rather about a more general and, indeed, disturbing lack of trust in politicians and the people charged with looking after our security—the Director General of MI5 and head of the Metropolitan Police. These people are not trusted when they
say they need these things. I think that is very disturbing, but it is not a reflection on the things they say they need.

**Q278 Lord Strasburger:** Do I take it then that you have no problem with content being collected as well?

**Professor Gles:** As you know, this is not about what; it is about who, when and where. Of course, content is a legitimate source of information but, again, as you know, people who want to intercept communications—that is to say gain access to content—have to go a completely different route. I think that is right. I think privacy is important. I am aware of Article 8 and the other aspects of the European Convention on Human Rights. That convention is extremely important but, in the real world of today, it seems to me entirely unacceptable that, like those people who rail against CCTV, people feel that they should be allowed to conduct criminal activities on the internet—that somehow it is a free space and it is a part of civil liberties and human rights that they should be able to use that free space for all sorts of wicked things from terrorism through to paedophilia and money-laundering. You know all the categories as well as I do.

**Q279 Lord Strasburger:** You would not be happy for content to be collected.

**Professor Gles:** Content is not addressed in this Bill. Yes, I am happy for content to be collected where it meets the very stringent different regulations that are required if content is to be looked at, i.e. a Home Secretary’s warrant. It has always been like that. We have had a secret service for more than 100 years in this country. It has always looked at these sorts of things. What has changed is everybody’s desire that this activity be made lawful and be brought into the law. That is very important. We need secret services. We give them a job of work to be done, yet they need to do it lawfully and they need to be accountable for what they do. As long as these things are all in place, I am perfectly satisfied.

**Q280 Dr Huppert:** I am struggling to understand some of what you are saying. When you talk about this being a philosophical question about the limits of state intrusion, actually it is what this Committee has to essentially determine and advise the Government and Parliament on. It is not just a sheer question of philosophy. You have been talking quite a bit about regulation of the internet and making things lawful online. I hope you realise that this is also not about regulating the internet, which is a different issue, involving a whole range of other Bills. It is that question about state intervention.

You mentioned people who describe this as a “snoopers’ charter” or who are concerned about CCTV. Can you explain to me how the argument that you made, either on the “Today” programme or just now to Lord Strasburger, would not apply to a proposition, say, to put a CCTV camera in every single room to monitor what happens, just in case it is useful? I think we would all agree that that would be quite useful in terms of reducing crime. I suspect, around this Committee and most of Parliament, most of us would agree that it was not the right thing to do. How does your argument differ from that?

**Professor Gles:** I am a professor of politics as well as somebody with a special interest in intelligence-led activity. I am sorry if I have confused you; that has not been my intention. As I say, I think the philosophy about what is private and public is a very difficult area. In Parliament, I do not have to talk about things that particular MPs may or may not have done.
on the internet to publicise their activities. When I came into this meeting on the train from Bicester North, I suddenly heard the voice of Boris Johnson booming at me.

Dr Huppert: You may have some issues about that, but that does not quite address the question.

Professor Glees: I will come to it; I just want to give you the context. The philosophical aspects of privacy are very important. Am I suggesting that there should be a Big Brother CCTV in every room? Of course not. In my view, the people who make this claim are living in cloud-cuckoo-land. If I may, I will just give you some statistics. In 2003, I wrote a book about the East German intelligence service, commonly known as the Stasi. If you have a look at a real surveillance society, which is what communist East Germany was, in 1989, the last year of the Stasi’s existence, there was one Stasi member to every seven East German citizens. In Britain today, there is one MI5 officer to every 7,000 citizens.

Q281 Dr Huppert: Professor Glees, clearly your book should be on all of our summer reading lists, but I still have not understood your principled argument as to why you are saying: “There is wrongdoing happening online; we could collect information about it, hence we ought to.” That is, as I understand it, the argument you are making, but the same thing does not apply when there is wrongdoing happening in rooms and we could collect CCTV information on it.

Professor Glees: The quick answer has to do with proportionality. Something does not become acceptable if it is done in private. A criminal act is a criminal act, whether it is done in somebody’s sitting room or whether it is done in front of Parliament here.

Q282 Dr Huppert: Whereas you were arguing that it should be done because it can be done and could be useful, you now say that in fact it is about the proportionality. Your argument is not about whether it is possible to collect this information online, from postcards or anything else, but whether it is proportional or not. Is that your new position?

Professor Glees: Sorry; I will repeat myself. When being interviewed by John Humphrys, or whoever it was, at 8.10 in the morning, you do not have time to develop a sophisticated argument. What I tried to set up was the point that there is this space; there are these things going on in this space. They are criminal things. It is now possible to at least have a go at finding out more about the things that are going on in this space. If it is possible, as it is, and if bad things are happening in this space, as they are, then it should be done. Of course it is a question of proportionality. If you are asking whether I think that councils should spy on people who put out the wrong bin, no, of course not. That is an absurd argument. It is the consistent attitude of what I would call the civil liberties lobby to reduce this argument to the absurd. This is not a matter of 50 shades of grey; this is something that is being done with existing communications. I am told that, every day, on average, each person in the United Kingdom sends four text messages.

Q283 The Chairman: Are they on criminal behaviour or criminal matters?

Professor Glees: I do not think they are on criminal matters, but I am just trying to make the point that this is a new form of communication that is being used. Thirty million people communicate with each other every day on the internet.
The Chairman: And you would collect all of it from everybody, because, somewhere out there, there are some people doing bad criminal things.

Professor Glees: Not only would I not do it, but it would be impossible to do it. That is the point.

Q284 Lord Armstrong of Ilminster: Many of us would agree that it was acceptable to have public authorities access communications data in the interests of pursuing terrorism or counterterrorism and serious crime, but the list of purposes is not 50 shades of grey but 11 or 12 shades of grey. Do you think that it is right that all of these purposes should be permitted by this Act? I know it is taking over from RIPA, so it already exists, but the Government appears to have shown some signs of wondering about that, because on the face of the Bill they have reduced the number of agencies that can collect and given themselves power to extend it to other authorities, so that people have to make a case. There is also the question of the purposes and some of the purposes are non-serious crime. Would it be justified or proportionate to use these powers for the pursuit of bicycle theft, which is a crime? Other purposes here are not criminal at all. Are you content with the list of purposes as it exists or would you like to change that?

Professor Glees: Well, Lord Armstrong, what I would say to that is what you have already said. These powers were in RIPA in 2000. By all means, one should always have a debate about what should and should not be looked at. I would say from my vantage point, on the one hand you have people like Sir Tim Berners-Lee, the father, as we all know, of the worldwide web, and adviser to the Government, who in April this year said allowing this sort of data-mining would lead to “the destruction of human rights”. Then you have people like me, who say that a human right is also to be secure. A human right is also to be able to walk down your road without fear of being mugged, or for children to go into a park without being accosted by drug dealers. Forty years ago, there may have been a copper on every street corner and in every public park. That is not the way it is these days. If CCTV, for example, can prevent crime and criminal activity then, yes, I am absolutely for it. On the question of proportionality, yes, I understand that, but again I point this Committee to things, for example, that David Davis MP has said.

Q285 The Chairman: Lord Armstrong was asking, of the permitted purposes, would you concentrate just on serious organised crime, terrorism and protecting the economic welfare of the state? Would you dump the other items on safeguarding public health and allowing people’s dead bodies to be found?

Professor Glees: I am happy with that.

The Chairman: Are you happy to dump the others?

Professor Glees: I am happy with it, but obviously the most important things are the things that come first—the things that involve serious organised crime, terrorism, paedophilia and matters like this.

Q286 The Chairman: Dr Richards, for Lord Armstrong’s question.

Dr Richards: I actually do have concerns that the range of purposes for which these powers might be used is too great. I would personally restrict it to serious organised crime including terrorism, and possibly certain emergency situations where lives are threatened, such as
kidnappings and so on. I personally feel that the complete list, in which there is provision for collecting taxes and so on, goes too far, in my book, because these are very intrusive capabilities and I am aware of privacy concern. Proportionality, for me, means that only the most serious of crimes are legitimate purposes for doing this.

Q287 Baroness Cohen of Pimlico: Either Dr Richards, Professor Glees or both of you, under current legislation, a large number of public authorities have access to communications data likely to be replicated using order-making powers. Are you concerned by the length of the list of organisations? Should the powers be limited entirely to the police and security? There is a fairly long list of other organisations. If you or Dr Richards think that the sorts of things you can ask should be limited, do you think the sorts of organisations that can ask them should also be limited?

Dr Richards: The short answer for me is yes; I think the list is too long. I think the capability is absolutely necessary, in my view, for preventing serious crime, including terrorism and so on. I do think there is a red line that this list perhaps crosses, in my view.

Baroness Cohen of Pimlico: Would you limit the list to police and security/intelligence services?

Dr Richards: I think I probably would, yes.

Professor Glees: Could I just say that I do not agree with my good friend and colleague? I think that victims of crime have a right to be safeguarded as much as is possible. It is very easy to say that fly-tipping, for example, is not a major thing, but if you live in a beautiful place, as my wife and I do, and it is defiled by people dropping their rubbish there with impunity, why should that be allowed? I am a zero-tolerance person. The argument that there are some things that are perfectly all right—you can beat your wife at home with all the doors locked so that nobody can hear the screaming, but you cannot do the same in the street—is anathema to me. I do not think lawmakers should be in the business of saying, to come back to David Davis, that the people who are going to be caught with this new legislation are stupid criminals. Criminals are criminals. Whether they are stupid or bright is of no concern to me.

Q288 Lord Armstrong of Ilminster: I share your views about fly-tipping, but is it appropriate for fly-tipping to use these powers to have access to communications data? I think that is the question that is in my mind. I would love to stop fly-tipping.

The Chairman: That was the question I was going to ask, but Lord Armstrong phrased it much better. We all want to take action against fly-tippers, but would you use the powers in this Bill to do so?

Professor Glees: You have to use the powers that you have.

The Chairman: Yes, but we are here to decide whether we should have these powers.

Professor Glees: Unlike my good friend and colleague Dr Richards, I am comfortable with them, but obviously, as always in life, you have to prioritise. There is a limited amount of people to do this. There is a limited amount of funds, and they should go to dealing with the most important issues first. There is no question in my mind about that.

The Chairman: It does not seem to have stopped some of the organisations in the 552 with access requests from finding the priority to do some of it.
Q289 Stephen Mosley: On those 552 organisations, there are only four listed on the face of the Bill. Do you think there should be more listed on the face of the Bill, or do you think that they should just come along afterwards through delegated legislation or something?

Professor Glees: Bearing in mind the public debate that has taken place, and bearing in mind that this is about the wellbeing of the public, the more that is set down and the more that is listed, the better. In a mature democracy, it is absolutely right to be having this sort of debate. Again, I pay my taxes, to the best of my knowledge, and I claim my expenses properly. If the use of communications data, which is currently not kept, would enable more people to stick by the law, I am in favour of it. This is the 21st century.

Q290 Michael Ellis: Gentlemen, can we come on to the issue of preventing inappropriate use of communications data? That is assuming, Professor, that you accept that there is a possible inappropriate use of such data. Would you accept from me that there is always a risk of misuse of power? We give constables the power to arrest people; there is always the possibility that that power will be abused. Here there is a risk of misuse. Would you say that it is proportionate to take certain risks in order to prevent crime and detect offenders? Would you say, therefore, that the terms of this Bill are proportionate? When coming to the issue of preventing the abuse, how would you propose to ensure that inappropriate use of communications is actually prevented?

Professor Glees: If I could deal with the second bit first—but I will come to the first bit—I think that the right way to prevent abuse is, first of all, to have proper regulation and a proper code of practice. As I said, I have read the Acquisition and Disclosure of Communications Data Code of Practice; I think it is a very good document and I am very happy with it. But there is another side, particularly where we are dealing with the secret world of intelligence. That is oversight and parliamentary oversight.

I am extremely concerned by what I regard as the failure of the Intelligence and Security Committee to play any role in this debate or, indeed, any serious role in any of the issues that have affected secret intelligence-led activity in Britain over the past few years. Our first port of call—by “our” I mean the public—should be to the Intelligence and Security Committee to find out whether the Intelligence and Security Committee and its Chairwoman are content with the appropriateness of proposed legislation. We are in a position, as I say, where we do not hear anything about that. That is why people like myself have to say the things that we do.

Q291 The Chairman: If I can elucidate slightly, I think you will hear, probably by 30 November, from the Intelligence and Security Committee, which will be conducting a parallel investigation to ours relating to the use of communications data for the Security Service.

Professor Glees: Forgive me if I say perhaps it has come 10 years too late, but better late than never. I know that it is proposed that the Intelligence and Security Committee be reformed. It is high time that it were reformed.

Michael Ellis: I think there is a White Paper about that.

Professor Glees: To go to your first point on the risk of people misusing the data, of course there is a risk. We saw it in the papers on Saturday: people can suffer because of wrong or unlawful behaviour.
Michael Ellis: You are referring to people who were wrongly arrested because of communications data errors.

Professor Glees: Yes, and that is wrong. Nobody in my position would seek, for one moment, to justify it. Just as the police will investigate people who are then found to be perfectly innocent, and that is not an argument for saying police should only investigate people who they know are guilty, so too, when it comes to communications data, we should not let the abuse of this in a very small number of cases indicate that this is not a worthwhile activity.

Q292 Michael Ellis: Briefly, Dr Richards.

Dr Richards: There are two things here and they are very important. One is the question of the capability that you have in place to extract the data. The second is the question of the process that you have in place for using that data. Sometimes, in a lot of the debates around this subject, the second aspect is forgotten or missed by some of the critics. There are some very rigorous procedures in place for accessing and using this data in a properly authorised way. Already there are procedures in place under RIPA that ensure, in my view, that, although there were always risks of misuse of this data or using it inappropriately, those risks are greatly minimised.

Michael Ellis: You would take the risk in order to resolve the mischief that the Bill is seeking to control.

Dr Richards: If you have in place a rigorous and appropriate process, then yes.

Q293 Michael Ellis: Finally from me on that point: do you think the penalties that are available are appropriate for those who would or could fail to comply with the requirements of the Bill? For example, for offences that might include the Computer Misuse Act, misconduct in a public office and the Data Protection Act, do you think those penalties are appropriate?

Dr Richards: Yes, I do, and I do not particularly see any need to change them. Those things are in place for a good purpose.

Michael Ellis: Do you agree, Professor Glees?

Professor Glees: Yes, I agree.

Q294 Mr Brown: May I just follow that up? You are both academics. You have made a study of this area. One of the great constraints on people taking part in wrongdoing is that they will be caught and punished. Are you able to say anything to us about people who take information from the police computer and sell it for commercial gain, or public servants who look up people’s social security or medical records and sell them for gain? Do you know how frequently this is done and how often it is prosecuted?

Professor Glees: No, it is not something I have done research into.

Dr Richards: No. Again, I return to what I said just now: there will always be risks that this can happen in a system. You have to put in place procedures and processes, firstly, to minimise the risk of it happening in the first place and, secondly, to monitor what is going on and to have the appropriate penalties afterwards, if that does happen. I have some personal experience of working in an intelligence situation where we used to make these sorts of requests for these sorts of data, previous to my academic experience.
Mr Brown: Do you accept that a principal fear in the minds of our constituents is that information about them will be improperly accessed, improperly used and may be improperly sold to somebody else? The biggest safeguard against that is that somebody who does such a thing will be caught and punished.

Dr Richards: I accept that people will have those concerns and I understand those concerns. Again, all you can do is try to reassure people that the appropriate procedures are in place to minimise that risk greatly and that people are held to account afterwards, if it goes wrong.

Mr Brown: You both believe that they are.

Dr Richards: I believe so, yes.

Professor Glees: You are talking about very serious offences. They are already serious offences. I would simply make the point to your constituents that their interests are better safeguarded in regulating this part of the cyber domain as far as possible. By “regulating”, I mean allowing it to be examined for the purposes of fighting crime. They are better served than by letting it be a kind of Wild West, where there is no lawfulness. People are far more likely to steal data from you or send you fraudulent e-mails if they think that they will not be traced. If they will be traced, they will not do it.

Mr Brown: I certainly agree on that point: that to make the law more effective, you have to capture people who break it and bring them to justice.

Lord Strasburger: We are talking here about safeguards against misuse. You both seem to be perfectly content with the safeguards that exist in RIPA. We have heard, in this Committee, of one known case of a prosecution, over several years, where there have been 0.5 million applications for data a year. Let us say that, out of 5 million applications for data, there has been one case of misuse identified. There are only two possible explanations in my mind, although you might be able to come up with another one. Either the safeguards are as immaculate and watertight as you seem to believe or the abuses are not being detected. Which do you think it is?

Professor Glees: For me, this comes back to the first point, which is trusting the people we charge to look after this area.

Lord Strasburger: Excuse me, but are the safeguards not there to check whether we are right to trust them?

Professor Glees: The statistic you have quoted, and I have not done the research into it, could be taken both ways. It could be taken to mean that there is a very small risk, or it could be taken to mean there is a massive cover-up and the public do not understand. I am inclined to believe that the people who do this—the head of the Met, the Director General of MI5 and the head of SOCA—do it with the right intentions.

In my experience, if I may say so, and in my work, if there has been a problem about intelligence-led activity in the United Kingdom, it has not been that it has been too interventionist; it has been that it has not been sufficiently interventionist. Things have not been found that should have been found. If you accept that and you accept that, in a lawful mature democracy such as ours, you have to place trust in the people charged with directing these matters, that statistic that you quoted to me bespeaks good news, not bad news.

Lord Strasburger: I am very happy to trust these people, but I am going to check to make sure that I am right to trust them.

Professor Glees: Of course there should be accountability. This is oversight.
Q297  **David Wright:** On that very point, clearly within the Bill it is not the head of the Met who is making a decision about what data is gathered. It is actually much further down the chain than that. Do you think that there is a need for more judicial oversight within the process? We have heard evidence already that requests for data inquiries really ought to be signed off, at least by a magistrate. Do you agree with that?

**Dr Richards:** No, I do not, for two reasons. Firstly, if the process is followed correctly, then, even though the authorisation is given within the public body itself, it should all be logged and recorded. Those logs should be available to the Interception of Communications Commissioner for auditing afterwards.

Q298  **David Wright:** Dr Richards, let me just break in there. What happens if you get an organisation with a canteen culture, where somebody goes along to one of their friends down the corridor and says, “I need some data on this particular individual or about this particular device and, I tell you what: don’t put it down under that level of request; stick it down under this box here, so that it does not show up on any monitoring report, so there is no data”? It comes back to this point about people abusing the system. It is far more difficult to do that if you have to present evidence before a magistrate, is it not?

**Dr Richards:** My experience is that, firstly, that sort of culture just does not exist in these bodies.

**David Wright:** What, nowhere? It does not exist in any organisation?

**Dr Richards:** I do not think it does. Secondly, if you have designed the system correctly, every request you make of an IT system is logged. Records are kept of what data you have pulled, when you pulled it and why you have pulled it, if it is designed correctly. I believe that you can design a system that can appropriately audit and monitor these things, if you design it correctly. The second point I wanted to make is that there is an operational imperative here. We heard the sorts of numbers of requests that need to be made to pull this data every year to support intelligence operations.

Q299  **David Wright:** Hang on. The scale for intelligence organisations is a separate point. We are not talking about the number of requests we have got. There is a lot of dispute about what those requests are for. One would imagine that, if there was some element of oversight from a magistrate, it would actually reduce the number of trivial requests for data, if I can use that phrase advisedly.

**Dr Richards:** It probably would, but I still think the scale of requests that the police and the intelligence agencies would be needing to make every day would be such that, for there to be judicial sign-off on every single request, the whole thing would grind to a halt operationally.

Q300  **Mr Brown:** Can I just ask it the opposite way around? Do you think that the magistracy is a sufficient safeguard and a necessary one just for the local government requests?

**Dr Richards:** Yes, although, as I said earlier, I am not entirely comfortable that local government should be using this data anyway.

Q301  **David Wright:** What we are saying is that a local authority has to go to a magistrate but that other organisations do not.
Dr Richards: I guess we are saying that, yes.

David Wright: And you support that.

Dr Richards: The implication from your question is that then you have a willy-nilly unregulated, unmonitored regime. That is certainly not the case. Procedures are in place to log and monitor. If the Interception of Communications Commissioner’s office is doing their job correctly, they have access to the details of every single request that is made and have the right to audit that at all times. There should not be provision for willy-nilly searching of data.

Q302 David Wright: Do you think there is the capacity in that organisation to deal with that?

Dr Richards: There needs to be. There should be. It should be built into the system.

David Wright: “Needs” and “should be” are different things. Whether it is is a different matter.

Dr Richards: I would take that as a necessity for this regime to be properly administered.

David Wright: Is it able to do that now, do you believe? On the basis of what is in this proposed Bill, would it have the capacity to deal with that now?

Dr Richards: Yes, it does.

Professor Glees: I think it probably does, yes.

Q303 Stephen Mosley: Clause 1 of the Bill gives the Home Secretary the power to specify what data is held, who holds it and what equipment they use, but it does not actually give any more detail of how they will do it or what they will actually ask for. Do you think it should be more specific there?

Professor Glees: In dealing with that question, it allows me to add my ha’p’orth to the answer that Dr Richards has given to the previous question, which is that I think that we need more oversight. There is no doubt in my mind about that. If members of the Intelligence and Security Committee should in future consist also of senior lawyers, I would be delighted—senior academics too, as far as I am concerned. The way this Committee is organised at the moment—that it lies in the hands of the Prime Minister to decide who should be members of it, any Prime Minister—I think is wrong. We all know that the police computer is, from time to time, abused by police officers. We know that. It has nothing to do with this new legislation; that is the way it is at the moment. That is wrong.

Q304 The Chairman: Professor Glees, sorry to interrupt you, but can I just clarify something with you? You said you need more oversight, and then you talk about the Intelligence and Security Committee. Less than 2% of the requests of the 0.5 million requests relate to the Security Service, so we are looking at 98% of these requests relating to ACPO and the police. Do you think there should be more oversight there, which would be the responsibility of the other Committee?

Professor Glees: I think that, as far as the acquisition and disclosure of communications data is concerned, yes, there should be more oversight. Generally, there should be more oversight over data-mining and formal interception. Who does it? As I say, we all know there is reform in the air; we do not quite know who is going to do it. That is part and parcel, as is accountability. At the end of the day, I think we have to trust the people we charge with doing this and there have to be very severe penalties when that trust is abused. It is my
understanding—I have not done a study of this but it is my understanding—that where police officers misuse the police computer, they are subject to very serious penalties.

Q305 Stephen Mosley: From that, in terms of this Bill, you think it should have a bit more detail—yes or no?
Professor Glees: Yes, more detail, absolutely.

Q306 Stephen Mosley: Dr Richards, one of the concerns we have heard about is in terms of black boxes. Is there any evidence to suggest that black boxes would be needed and do you have any concerns about introducing these into the mix?
Dr Richards: There are two elements to this issue. One is a technical element, and I will confess straightforwardly that I am not a technical expert on telecoms networks. The other is a risk and security issue. On the technical issue, my limited understanding is that, because the telecoms network is becoming so dynamic, diverse and complicated, the way this data could have been collected before, when you had particular pipes that everything went down and you could put a tap on to them, is no longer technically feasible. Stuff is flying around all over the network in a very dynamic way. I believe there are technical reasons why a more dispersed system of collecting this data is necessary but, as I say, I am not a technical expert and you would need to speak to other people about that.
In terms of risk, clearly any situation where you push sensitive equipment—and this is obviously sensitive equipment handling sensitive data—and disperse that greatly out of secure locations and into the telecoms network, yes clearly the risk goes up that something will be compromised, hacked into or there will be privacy issues. We have to weigh the balance of the technical need to do this in a particular way and the need to protect it as far as possible.

Q307 Stephen Mosley: One of the other new innovations within this Bill is the filter. What are your views on the creation of a filter? Effectively, to me it sounds like a search engine, which effectively will mine all the data that is out there and almost make it into one virtual database. Is that your opinion and do you see any risks with that?
Dr Richards: To the front end, to the analyst who is pulling the data, yes; in a way it will look and feel the same. By using this filter mechanism, it will look and feel the same as if there was a great big database behind the scenes that you could dip into to pull the particular information that you want. However, for operational reasons, it does not seem to make any sense. These intelligence questions that are being asked of the system about people’s communication behaviours and patterns are quite complicated questions that require several different pieces of information to be pulled together and analysed, in a fused way. It does not seem to make sense to make that as difficult as possible, by saying you have to get this bit from over here, then you have to get this bit from over there, then you have to get that bit from over there. That just reduces our intelligence capability to the benefit of the terrorists and the criminals that we are going after. I think it is null issue in a way. If you are collecting the data, then how you query it, to a certain degree, to me does not pose any more risks than anything else.
Q308 Stephen Mosley: I can see some advantages to using a single filter to do these searches because, as you said, it provides one place for security, for auditing purposes and for logging purposes. Would you think that that would be an advantage?

Dr Richards: Operationally, it would be a massive advantage. Yes, that is what you need to do at the end of the day; you need to combine lots of different pieces of data together to give you an intelligence picture of what you are looking at.

Stephen Mosley: It might be an advantage to channel all the inquiries through the filter. I think, looking at the Bill, it is saying that they will do the inquiries normally, but only more complicated ones would be put through the filter. Do you think there would be an advantage to having only one access point effectively, which would be the filter?

Dr Richards: There probably would be, for all the operational reasons that we have discussed.

Q309 Stephen Mosley: Lastly, the Bill gives the power to the Secretary of State to transfer the ownership, the maintenance and the running of this filter to a third party. What are your thoughts on that?

Dr Richards: Again, it may be a technical question. I will refer back to some of the comments I made earlier. As long as you have the appropriate authorisation process and monitoring regime to ensure that everything is being done in a legally compliant way, so that you can monitor and audit logs to make sure that people are using the system appropriately, then I do not necessarily see a problem with that. It may be that the Secretary of State’s office is not the best place, technically or logistically, to be able to run this system anyway. As long as you have the sufficient safeguards in place, I do not necessarily see that this is a problem.

Q310 The Chairman: Dr Richards, the Home Office has called it a filter, giving the impression it is narrowing down the information sought. I think Mr Mosley has called it a search engine, giving the opposite impression. Whose description is the more accurate, in your view—a filter or a search engine?

Dr Richards: My understanding of it is that “filter” is a slightly inaccurate word for this, because you are filtering lots of different pieces of information out of the system and putting them together.

The Chairman: Mr Mosley is right: it is more of a search engine, in your view.

Dr Richards: That is my understanding of it, yes. That is actually a more accurate description.

The Chairman: You agree as well, Professor Glees.

Professor Glees: I do, yes. I am not technical at all, but it is my understanding that a filter does exactly as Mr Mosley says.

Q311 Dr Huppert: You have both looked at approaches to communications data collection in other countries. There are a variety of different approaches. Are there any around the world that use the approaches proposed within this Bill?

Professor Glees: My understanding is that the Australian Government is closest to the United Kingdom in terms of this particular Bill. The country that I know most about, apart from the United Kingdom, is the Federal Republic of Germany. There, the German Chancellor is on record as having said, in her view, Germany needs similar legislation.
**Dr Huppert:** As I understand it, Germany currently does not have any aspect of the data retention directive, so they are somewhere behind and trying to catch up to where we were years ago.

**Professor Glees:** For historical reasons, not just because of the Nazi past but also because of the Stasi past, this is a very much more difficult issue in the Federal Republic than it is in the United Kingdom, where we look back with pride on our long history of democracy.

**Q312 Dr Huppert:** Indeed we do. Germany is way behind and would like to catch up to where we are now. You say Australia is sort of roughly where we are but trying to move a bit forward. Are there any countries around the world that currently collect communications data, or try to collect communications data, in the way envisaged in this Bill?

**Professor Glees:** To the best of my knowledge—I suppose the moment I say this someone is going to disprove it—there is no proper research into this. The distinction that would be made would be between the 27 member states of the European Union and the states of the European Economic Area, which share a common understanding of this problem, and then countries outside there. Obviously in a place like North Korea you would expect that they would take a very different attitude. That is why I come back to saying this is about lawfulness in a mature liberal democracy.

**Q313 Dr Huppert:** I suspect North Korea would say similar things about lawfulness. Do you agree, for example, with Joe Biden, the Vice President of the United States? He argued that, where you have monitoring arrangements like this, which impose some technological drag through back compatibility and various other areas, they might lead to businesses moving elsewhere in order to avoid them. As long as there is a difference in different countries as to what you have to do, there is an incentive not to be covered. Do you think there is a risk that companies may choose not to be in the UK, to do less activity in the UK, to store data overseas or something like that?

**Dr Richards:** I personally do not think there is a big risk there, for two reasons. One is that the telecoms network is a global network. It is very dynamic; it is very transnational, not just technically but in terms of its management as well. Whether you locate in one country or another kind of becomes less significant technically. Also, there are other reasons why, as a telecoms company, you might want to locate in the UK. There are particular fears about this interception capability, particularly given that it is supposed to be Europe-wide, and I know that lots of other EU countries are way behind in implementing this.

**Q314 Dr Huppert:** Just so I understand, you are saying the system is incredibly dynamic and so telecoms companies could easily move, but they will not choose to do so, so does it not weaken our benefits? If you are saying there are economic benefits to being here, does it not at least weaken them?
**Dr Richards:** What I am saying is I do not think you do sufficiently, because there are other reasons for why you would locate in one or other country that greatly outweigh that issue.

**Dr Huppert:** You weaken them but not enough. I think I understand that.

**Professor Glees:** I think there is an ethical dimension here that should not be forgotten. That Mr Biden may have made these comments as an American does not impress me. We have seen a big company like Amazon, for example, managing to avoid paying tax anywhere in the world, as far as one can tell. This again is a consequence of the lack of regulation of the cyber domain. I would argue strongly, looking maybe at the banking crisis and various other things going on, that the idea that unregulated space leads to economic success is extremely dangerous.

**Q315 Dr Huppert:** Again, Professor Glees, we are not talking about regulation; we are talking about data collection, which is very much not the same as regulation.

**Professor Glees:** To me, regulation means the imposition of legal norms and laws. That leads to regulation.

**Dr Huppert:** Professor Glees, the laws still apply; the question is about how you collect the information, which is not the same as regulation. A room that does not have a CCTV camera in it is still subject to the same laws as one that does. It is still regulated in the same way; it is just a question of what tools you have to go out and collect the information.

**Professor Glees:** It is a good philosophical argument but, as I say, the American pressure, which is that somehow, of all forms of communication, the internet should not be subject to lawfulness, I would say, is not something that should be seen as being of great economic advantage, except to the particular companies that are able to exploit it. We have seen where that ends.

**Q316 Dr Huppert:** We will hear what a number of the companies have to say about this later. Do you think there is a risk that, when you collect data into any sort of database, whether it is a central one or a number of other ones, you create a honey pot—that there is an incentive now for people to try to attack that data to get hold of it? Do you accept that as a risk—that you are generating a new source of crime?

**Dr Richards:** In terms of cyber-crime you mean?

**Dr Huppert:** Yes.

**Dr Richards:** Potentially, yes, but it is a risk you have to consider against the benefits that you get from accessing the data. Again, going back to that technical point earlier about whether, if it is implemented in quite a dispersed way, you disperse that risk, if it was all sitting in a lovely nice database in Cheltenham or wherever it may be, in some ways that risk would be higher.

**Dr Huppert:** There is a fascinating tension between one very secure location and a number of potentially less secure locations, and I think I understand the argument.

**Professor Glees:** The starting point is that the crime is out there. The crime is not made by the fact that this is data that can be mined. That does not make the crime; the crime is there. Mining the data might diminish the crime.

**Q317 Baroness Cohen of Pimlico:** Can I start with Dr Richards? People always suggest to us that, whatever regime is put in place, criminals and terrorists will evade it with the utmost
ease. Since your background has to do with terrorists, do you think that is right and, if so, is there any evidence that shows they can evade this? That is what I am after.

*Dr Richards:* Yes, criminals and terrorists are very well aware that they are being monitored. They are the masters at trying to evade such monitoring, as far as they possibly can. That has happened throughout history. The suggestion that criminals and terrorists could easily outwit these sorts of mechanisms is greatly exaggerated, in my view. The only way to really avoid being monitored by the authorities is not to use any electronic communications at all. That is the only way you can be sure of doing it.

*Baroness Cohen of Pimlico:* Back to the carrier pigeon.

*Dr Richards:* Absolutely. Yes, there are ways. One of the things about the internet is you can appear on it very anonymously, but people have to communicate; they have to use the services that are there, otherwise nobody knows who is talking to whom. I would say there is a limit. Yes, they will make it as difficult as possible, but they will not make it impossible to be tracked, in my experience.

Q318 David Wright: We have heard quite a bit of evidence from the Home Office team about monetary costs and benefits from these proposals. I would welcome your thoughts on them. We have heard estimates that the cost of the draft Bill will be £1.8 billion over the next 10 years and there would be £4.4 billion of net benefits. What do you think of those costs and benefits?

*Professor Glees:* I am not able to comment, I am afraid, on that aspect of it. All I would say is that estimates of costs and benefits are always going to be matters of speculation. That is all I would say; I have no expertise.

Q319 David Wright: Dr Richards, have you got any experience on this?

*Dr Richards:* I would broadly say the same. From a technological point of view, the proposals that flow out of this Bill are technologically very complex. To be able to do this physically entails some cutting-edge technology, which probably will cost a large amount of money, probably in the order of billions rather than millions. Whether it is £1.8 billion I just could not say; I just do not know.

Q320 David Wright: We have heard suggestions this afternoon that it would be up to 10 times more than that.

*Dr Richards:* I just could not comment on that. If we are talking £18 billion, that seems an extraordinarily high figure to me, but I just do not know what it would entail. In terms of the benefits, again I am extremely suspicious of any official figures on this. I think it is impossible to put a figure on how much you save the country by winding up criminal enterprises, capturing terrorists and so on. We see all sorts of figures bandied about. The National Security Strategy said that the annual cost to the UK from crime is £1 trillion. Where that figure comes from and how they have calculated it I just do not know. Particularly when we are looking at cyber-crimes, given that we do not know how much cyber-crime is actually going on, how you can put a figure on it I do not know. This is a very fraught area and, in my view, anyone who gives you an accurate figure is dubious.
Q321 David Wright: You are not aware of any academic modelling that has been done outside of the Home Office or other government departments on the benefits of this type of activity, more broadly.

Dr Richards: I am not aware of that, no. In fact, the only academic debate I am aware of is the fact that you really cannot trust any official figures on this.

Professor Glees: I think one policy aspect of cost is that any Government needs to be cautious about private industry trying to sell it software, at huge expense, that claims to do the filtering that we have talked about. In our own work, we are aware of the pressures on Government from what used to be called the military/industrial complex—the big companies that are very busy wanting to sell stuff. In respect of that, without trying to put an inappropriate plug in for our own work at the university, there are some things that the state has to do. The provision of security is one of the things the state has to do. The people who need to do this sort of work should be properly employees of the state and trained to do that. I do not think this is the sort of technical work that should be farmed out, because that would be a huge cost and a huge expense. To the best of my knowledge, both our Security Service and the Government Communications Centre and busy trying to recruit the young talent that they think can do this sort of work at the moment, and I think that is the right way to approach it.

Q322 The Chairman: Professor Glees, could I take you back to the point you have just made on being suspicious of suppliers willing to supply the sophisticated kit? As I understand it, one cannot go to PC World and get a range of this. There will be a monopoly supplier doing a specially designed bit of special kit. We all have experience of Ministry of Defence contracts that go to two, three or five times the cost, and then the generals always want to add an extra button just before the thing is delivered, putting the cost up again. Have you a view, therefore, on a monopoly supplier of this equipment? Are you suspicious of the cost estimates?

Professor Glees: Yes.

Dr Richards: Yes. As I said earlier, you are absolutely right that this is an extraordinarily complex technology that you cannot buy off the shelf. There are cost implications in that and cost risks for the Government.

Q323 David Wright: I am not a technical expert, but presumably this piece of kit will have to interrogate different private sector databases, which may be constructed in different ways. It will have to be adaptable to a number of private sector organisations’ structured databases.

Lord Strasburger: Which are changing all the time.

Dr Richards: My limited understanding is that, yes, there is a huge array of different types of data, which is the problem, but the data rates are the problem. The amount of data flowing through the network is extraordinarily high and right at the upper limits of current computing technology. Those are the sorts of issues that you have got here.

Q324 Stephen Mosley: Has any assessment been made of how much data will be collected over the period of one year?

Dr Richards: Not that I am aware of. I would imagine, within the appropriate parts of government, within GCHQ and so on, they would have some sort of estimate of this. Whether that is disclosable, I just do not know. I have not seen anything publicly.
Professor Glees: Of course, we know the figure for last year, which I think was 550,000 requests to examine data.
Stephen Mosley: That was not the question; it was how much data is being stored over this process.
Dr Richards: I would think that would be known. The telecoms companies themselves know how much data is flowing over their networks, but I do not know. It is a lot.

Q325 The Chairman: Dr Richards, would you be aware of which countries in the world would be capable of making these black boxes and this sophisticated kit?
Dr Richards: Some of this gets into quite sensitive technologies, which I am not qualified to comment on. There would be a small number of countries that could do that.
The Chairman: Do we have the capability in the UK, do you think?
Dr Richards: I believe so, yes.

Q326 Mr Brown: Do you believe that, eventually, there will be an overarching European Union regulatory regime in this area? Do you believe the approach that the last Labour Government and the current coalition Government are taking, because they are broadly similar, would be compatible with what is emerging from the European Union?
Professor Glees: It is my understanding that the answer to that is yes. It is a critical area of cooperation with our European partners. Of course, if we were to leave the European Union, as some people say, that is something you could throw out of the window, but at the moment we do seem to be, all of us, talking the same kind of language, subject to the same kinds of directives and underpinned by the same convention on human rights. That is good, in my view.

Q327 The Chairman: Unless any colleague has got any other question, could I conclude with this one? I think, Professor Glees, you said, “Of course, subscriber data is only who, what, where,” but as I seem to be learning, it is not actually just who, what, where; it is who, what, where, when, the details of your bank account, every single thing you may put on your private Facebook account, your home address—everything under the sun could technically be subscriber data. Is that correct?
Professor Glees: I am afraid, if I said that, I misspoke. What I thought I said was that what this is about is “who, when and where”, but not “what”.
The Chairman: Sorry; my apologies. Yes, you did say that.
Professor Glees: I know people in the civil liberties lobby say, if you are looking at “who”, you are looking at “where” and you are looking at “when”, you are bound to also see “what”, but again I have trust in the people we charge to do this. They say that it is not about “what”.

Q328 The Chairman: I accept that. Let us forget about the “what”. I misspoke there, if I said “what”. What I was trying to get at is that subscriber data, as I understand it, is not just who, what, where. It is not just the person’s name and their telephone number; it is a huge range of material, including your bank account number, including all of the information that you have to give to Vodafone, Virgin, Facebook or Twitter when you sign up. That is subscriber data.
Professor Glees: Yes, absolutely. Again, we know that that kind of data not only exists but is most massively exploited, not by any government agency or council or authority, but by the people who sell things to you on the internet. It is a fact of life.

The Chairman: For business purposes. That is a different question. Can we be clear then that, when we say, “Subscriber data is only who, what, where,” it is not technically just who, what, where? It is who, what, where and an awful lot of other stuff.

Professor Glees: My concerns are related to this proposed Bill, and there it is very clearly stated that this is not about “what”. One can believe or not believe it as one chooses. I choose to believe it.

Q329 Lord Armstrong of Ilminster: I think I got from the previous session objections from the civil liberties people that the “what” included so many things that it was tantamount to content. Of course, it is the “what” that gives the authorities the clues that they want to pursue their criminal investigations. Have you any thoughts about the point that the Chairman makes about the extensive subscriber data and the borderline between that and content?

Professor Glees: Where the civil liberties lobby, if I could describe them thus again, come at this from is the idea of a snoopers’ charter and a surveillance state. For them, the starting point is that there is this great bank of data that will be mined arbitrarily, and that will affect each and every individual. If you come at this from the point of view of the Government and the agencies, this is about particular searches for people who may be involved in serious crime, or may be threatening suicide or risk of life. You all know the categories. There it is about finding about with whom they have communicated, when they have communicated and where those communications have taken place.

Lord Armstrong of Ilminster: Which tells you something about what they are talking about—or may do.

Professor Glees: The “what” will trigger the specific investigation, but what is being mined is not the content, generally. It is not a surveillance-state operation; it is a targeted operation.

The Chairman: Unless you have any other comments there, Dr Richards, thank you once again, gentlemen. We have grossly exceeded our time with you as well. I am sorry for keeping you back so late, but thank you very much for again an excellent evidence session, which we will chew over carefully. Thank you very much.
TUESDAY 4 SEPTEMBER 2012

Members present:

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

Professor Ross Anderson, Professor Sadie Creese, Professor Peter Sommer and Firewolf [Glyn Wintle] (QQ 330-416)

Examination of Witnesses

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.

Q330 The Chairman: Welcome, lady and gentlemen. I am sorry you are so far away in this mega room. I can barely see you down there. I hope the acoustics are okay, but please speak up. We are now in open session. We have read your evidence, Professor Sommer and Professor Anderson. I apologise for the fact that you were not heard back in July. Our session ran on longer than expected. We had some excellent evidence to hear so we had to defer your evidence. You are very welcome before this committee today.

Before we start, it would be helpful if each of you would say, very briefly, who you are and then we shall crack on with the questions.

Glyn Wintle: I am Glyn Wintle. Of particular interest to this committee is the fact that I get paid to break into computing systems to check their security and I am involved in cleaning up government data.

Professor Sadie Creese: I am Professor Sadie Creese. I am professor of cybersecurity at the University of Oxford.

Professor Peter Sommer: I am Peter Sommer. I am visiting professor at De Montfort University and visiting reader at the Open University. Most of my income comes from acting as an expert witness in these sorts of cases.

Professor Ross Anderson: I am Ross Anderson, professor of security engineering at Cambridge. I also chair an NGO, the Foundation for Information Policy Research, in which
capacity I was involved in lobbying and advising the House during the passage of the RIP Bill a dozen years ago, as you may recall.

The Chairman: Thank you very much.

Q331 Dr Huppert: I welcome all four of you. I shall start by asking a few questions about the distinction between communications data and content. The Bill currently assumes that a clear line that can be drawn between those two. We have had some evidence, particularly from Professor Sommer and Professor Anderson, that that may not be the case. I would be interested to hear from all of you whether you think there is a very clear distinction between those two or whether there is, in fact, a very grey area linking them.

Professor Peter Sommer: First you have to understand that you have to apply two tests. The first is a legal test: what does the legislation actually say? Until you have a very clear idea of what the law says in terms of what is communications data and what is content, you cannot try to translate that into a series of technical measures—filtering of the sort that is being suggested in the legislation. Many of us believe that the definitions are far from clear. They were clear back in 1985 with the Interception of Communications Act, when essentially all one was talking about was telephones and the content of the voice element and the telephone bill plus the subscriber information was the communications data. In RIPA, they tried to extend it, but there were various sorts of understandings about what things were supposed to mean, and that is still rather unsatisfactory.

I draw to your attention a report produced by Justice in October 2011, called Freedom from Suspicion, in which they looked at the definition of communications data and the definition of intercept. They also drew attention to the circumstances in which the Home Office has had difficulty in defining that. Before you even get on to the techie stuff, the first thing is whether you can help the techies know what they will be doing at a practical level.

I see you want to interrupt, Dr Huppert. Please do so, but I would like to follow on and talk about the technical position.

Q332 Dr Huppert: Before you move on to the technical aspects, could you give us an example of where that grey area is and where you think the legislation is currently unclear?

Professor Peter Sommer: Let us take the definition of use data. Communications data consist of traffic data, subscribed data and use data. If we look at the definition of “use”, it says that it relates to how a subscriber uses a communications system, but it excludes content. Take the example of Google, which collects prodigious amounts of information about how we use their service—which after all is their fundamental business model—and where exactly do you draw the line? I am not doing this for some sort of stagey effect; I have absolutely no idea how that will be done. It seems to be a bad principle when making legislation if you know in advance that you are going to have to rush off to the courts for assistance.

Q333 Dr Huppert: Do you want to move on to the technical aspects and then I will see whether any other members of the panel have anything to add?

Professor Peter Sommer: Let us move on to the technical aspects. As I think that most members of the committee will know, communication on the internet takes place in a series of packets. Each packet contains information about where it has come from, the IP address of the originator, the IP address where it is supposed to be ending up and some supervisory
information, so that if the packets arrive slightly out of order, they can be reassembled. The rest of it is what we call the payload. The payload, for RIPA purposes and the purposes of this Bill might be content or communications data or simply flags or pointers which tell you what will happen afterwards.

If you are carrying out a technical analysis using deep-packet inspection kits to carry out an investigation, you cannot look at it on a packet-by-packet basis, you have to collect a series of packets and may need to reassemble them back into webpages to understand what is going on. It gets more complicated than that. First, let me say what the challenge is. Mostly, when you are using DPI kit, you are carrying out a specific investigation—you are using it to find out if somebody is committing a fraud, if a computer system is being attacked, if a piece of equipment is misbehaving—so you know what you are doing.

In this instance, the CSP is not carrying out an investigation, it is carrying out the requirements of legislation to separate communications data from content, so the requirement on the kit is absolutely fantastic. That is why it costs a great deal of money. Finally, a lot of this data is encrypted, so only small parts of the packets will be visible and understandable. The CSP will know that both content and communications data have gone through, but if it is encrypted, it will not know why. The encryption is not to thwart anybody, it is to protect the end user from routine eavesdropping. I apologise for my long answer, but I hope that that will help people get the big picture.

Q334 Dr Huppert: Do any other members of the panel have things to add? We do not need to hear the same information again, but is there anything that anybody wants to add?

Professor Ross Anderson: There are three, or perhaps four, difficult use cases that the committee should consider. The difficult case during the RIP Act was: what happens if someone goes to Google and types in “pregnancy test”? Is the traffic data “… google.com” or is it “… google.com/query pregnancy+test”? We had a big debate in Parliament that came to the conclusion that traffic data was just up to the first slash.

However, the world has moved on. The next use case is of augmented reality. As we walk around with our mobile phones, we come to a shop. The shop has a QR code offering 10% off. You go “beeb” with your phone. You scan the QR code. You have gone to that website. As you walk around the street and interact with reality, your traffic data, your communications data, is not just a history of your location, through your cell site location history, it is also a history of your attention. That is the very click stream, the very attention stream, that Parliament decided in its wisdom 12 years ago that it was not going to give to the police as communications data. Now the set of websites that you visit will evermore give away your attention sequence. Once you have Google Goggles and they start recognising people you know, so I look at Julian and I see Julian’s website and when I look at Nick Brown, I see Nick Brown’s website, that is all communications data. It contains what I have looked at and who I have looked at.

Finally, in the research labs, the distinctions are about to be abolished because, as we have moved to software-defined networks, it may no longer be packets that we are moving around but cache lines, streams or data at other levels of abstraction.
Q335 Dr Huppert: Professor Creese?

Professor Sadie Creese: I think that my learned friends have all made excellent points. However, technically, it is still feasible to create a definition of communications versus content, but we have to recognise the challenges that my learned friends have laid out for us—that it will not be straightforward. We will witness a blurring of what may have historically been considered to be in the realm of content data which will now crop up as communications data. That does not mean that it is technically unfeasible to create those definitions; it will be technically feasible.

Dr Huppert: Do you think that the draft of the current Bill has a grey area?

Professor Sadie Creese: I think that there are many difficulties with the draft of the Bill. If I was to try and sum it up succinctly I would say that, in some ways, it is because it inherits so much terminology of telecommunications—in fact it is littered with references to telecommunications service providers—and yet many of the organisations and many of the digital-based services that the Bill is trying to reach out to are run by organisations that will not perceive themselves to be in the business of telecommunications. If somebody is running instant messaging, is that telecommunications or is that cloud services? Are cloud services telecommunications in the context of the Bill? There is an awful lot of language that may still be out of date, and some work needs to go into bringing this up to date with, as Ross has mentioned, augmented reality. There is an awful lot of functionality-rich content that the Bill does not directly address although it probably should, and could do a better job of.

Q336 Dr Huppert: Perhaps I could take Mr Wintle. He has not had a chance.

Glyn Wintle: I would break it into two separate parts. There is the difficulty of separating the content if you are the communications provider and you are willingly involved in the process. For certain types of communications that is doable; for other things, for example, in Second Life, what is communication if someone comes and drops a parcel in one place and somebody else picks it up? Am I as the maintainer of Second Life meant to log all these movements of these objects? People ask, “What to what?” If so, the cost of this is enormous.

The second one is, of course, when you are using the black boxes and trying to do the interception, absolutely, categorically, you are going to get some blurring. Some of the stuff that worked one day did not work the next day, and so some of the data that you think is perfectly valid and has this isolation will not, even if you do everything perfectly and an ideal world exists, which is does not.

Q337 Dr Huppert: Professor Anderson, in your submission you talked about the possibility that although this Bill quite explicitly says that it would not allow any interception under the Bill, none the less the equipment that could be installed and paid for with the £1.8 billion could itself be used for interception once it is already doing deep-packet inspection. Is that a concern that the rest of the panel would share—that this could be a way that essentially the Government is paying to have more interception capability even though interception is nominally not in this Bill?
Professor Peter Sommer: It is not particularly my view. If you go along and look at RIPA—I do not have all the details of RIPA permanently imprinted on my brain, but I think that if you look at Sections 5 and 8, which cover certificated warrants, then in essence that gives the Foreign Secretary, in this case, the power to give quite broad warrants to GCHQ to carry out interception. Taken together with Section 12 of RIPA, which is concerned with requiring CSPs to put in interception facilities, my guess is that the legislation route is all there. It is then really a question for the Director-General of GCHQ to get extra funding for whatever he believes is necessary and to persuade presumably the JIC of the correctness of his view.

Q338 Dr Huppert: Anyone else?

Professor Sadie Creese: I felt the Bill was clear on this point. No technology exists without controls and balances around it and due process etc. I would recommend that, in evolving the Bill, further attention be put in those areas in general, not just on this point but as a safeguard.

Glyn Wintle: On the exact question you are asking, the Bill is not clear on this point. It says that we install the equipment and what the equipment should do, but it does not say that the equipment should not do something else as well, although that would have to be covered by law. If the equipment that is put in is a general purpose computer and therefore can do anything—and in fact it would probably be harder to make the equipment not be able to do interception, or at least to have the ability to be reprogrammed to do interception. In fact that is probably a big concern that somebody else uses the hardware for purposes that it was not originally intended for, and not necessarily a Government.

Q339 Dr Huppert: Professor Anderson, perhaps I can ask one last question. You have suggested that we look at a particular ETSI document “Lawful Interception … Cloud/Virtual Services”. Perhaps you could say a word or two, in layman’s language, about the issue around that as well as comment on the interception issue.

Professor Ross Anderson: The issue comes around every few years, whichever Government is in power. GCHQ wants more capabilities and it wants its capabilities upgraded. Clearly it has been felt appropriate to talk about communications data primarily in this Bill. If you want to know what the technical people are doing, the place to look is the ETSI documentation because that is the forum that sets the technical standards for interception. In the early days of mobile telephony, the telecoms providers had a lot of bother because Britain came along and said, “Please provide the following interface to our surveillance systems”, and the French and the Germans would come along and the whole engineering business became unmanageably complex. We said, “Fine, we have a telecoms standards institute; we have a committee that does lawful intercept; we will have the telecoms, we will have the intelligence agencies and the equipment suppliers sit round the table and decide exactly how a spy agency computer or a police computer should talk to a phone company computer”. If you want to know what the real long-term intent is, that is the place to look.

It is clear that the agencies, not just in Britain but overseas, are thinking not merely in terms of automatic access to ISP equipment, but also to the equipment of firms like Google and Facebook. If you get up in the morning and check your Facebook account from home and then on the Tube from your phone and then at work from your desktop, it is an awful lot easier to follow you through Facebook systems than it is to follow you through the systems of
several different CSPs. I believe that you are seeing Google and Facebook later on in this process and no doubt you can discuss that with them.

**Professor Peter Sommer:** There is a slightly more benign interpretation. I have used ETSI standards in cases overseas related basically to telephones and not to data communications. There is an equal emphasis, in this more benign view, on both “lawful” and “intercept”. In other words, there is the problem of how you carry out an intercept but it is also necessary to be able to do it in a lawful fashion; in other words, you are creating a record of what has been done. If we look at the telephone standard, in essence what you get in a single record is the authority under which the interception is taking place which you can link back to a judicial decision—we are talking about what happens overseas and not what happens in the United Kingdom. You can then get the call data records, which is your telephone bill, but you also get embedded in the same records the voice component as well. The idea is that you end up with something that is evidentially robust. I am not contradicting what Ross is saying, but I am suggesting that one of the purposes of the standards is that equipment internationally is more or less the same because that helps the exchange of evidence and makes it reliable. It also means that different countries do not have to specify their own equipment. I hope that assists.

In relation to the cloud thing, I think one can also read it benignly as trying to design a means of capturing evidence from the clouds in a sort of evidentially robust way as well.

**Q340 The Chairman:** I was also fascinated by the comment—it probably was in Professor Anderson’s paper—that, if we looked at ETSI, we would see what the real game plan of the Home Office was long term. I understand that it is all technical and that I would not understand a word of it. Professor Anderson, is it possible to identify, in layman’s language, from the ETSI document what that long-term game plan is, or is it merely that they want the highest level of equipment possible that, one day, may be used for more intelligence gathering purposes?

**Professor Ross Anderson:** The game plan that becomes apparent from the ETSI document is that, on the one hand, they want a lot of deep-packet inspection equipment so that they can look at communications which go via services to which they cannot get back-door access, but they would greatly prefer it if they could get back-door access to the services that we use to communicate.

**Q341 Ten years ago, electronic communication tended to be end-to-end—e-mail from my PC to your PC—and then the policy concern was, “Suppose we encrypt it; what would the Government do about that?” Nowadays, the big change that has happened is that most communications between people involve some other service provider, be it Twitter, Facebook, Gmail, Yahoo or hundreds of firms that are just being set up. The logical thing for the agencies to do is to go to Mr Google and say, “Knock, knock, here’s a warrant, please tell me everything about Mr Brown”. The problem is that the service providers are global and do not necessarily know the nationality of the users or their domicile or their residence or where they happen to be now. That slows up the whole operation because if someone says to Mr Google, “Knock, knock, please give me Mr Brown’s Gmail address”, Mr Google’s lawyers will quite properly want to ensure that he is a UK citizen, that he is a resident, that he is physically present here and that it is not some trick to get hold of information to which the UK Government or some other government are not entitled. So service providers give the
potential for much greater coverage, but that brings with it enormous complexity and difficulties both technical and legal. That is what ETSI is focusing on.

The Chairman: If you could send us an a short paper backing up your view that the real game plan at the Home Office can be revealed in the ETSI documents, I would like to see the relevant bits of the ETSI documents which justify that and your analysis of them, if that is possible. We will not do that today, though.

Q342 Baroness Cohen of Pimlico: Thank you, Professor Creese. I have at last grasped why I am having such difficulty with this subject. The Bill and I are using the language I understand, which seems not to relate to the subject. Is there a way that by changing the language in the Bill, the whole thing will fit more closely with what is going on on the ground? If the language does not fit, you are going to be lawyered all over the place. It will become unglued immediately you get to the courts.

Finally, thanks to Professor Creese, having grasped what is wrong with my perception of the subject and, as a lawyer, what is going to happen when we get to the courts, I am seriously worried.

Professor Sadie Creese: Yes. I think it is possible to fix, but you need to be aware that as soon as you attempt to do that, you will open a floodgate of issues. What is the nature of things that are not typically telecommunications? What does the data consist of? What are the practicalities of achieving this filtering functionality? Having read some of the evidence you have already taken, I think that people have already raised with you the complexity and how it relates to cost. But I maintain from a technical standpoint—

Q343 Baroness Cohen of Pimlico: That it is doable.

Professor Sadie Creese: It is possible, yes, but you need to be prepared for that debate to widen as soon as you do it. The language in the Bill is so constrained at the moment. Once you embrace that opening up, I think that you will find that there are other things to be dealt with it, including the complexity of the governance that you place around it, the processes, how you monitor the automation that you are putting in place, what should be the proper auditing—it is certainly not annual.

Q344 Baroness Cohen of Pimlico: Is my suspicion broadly correct that by trying to extend this to foreign CSPs we have opened a Pandora’s box?

Professor Sadie Creese: That is a completely separate and challenging issue, because cyberspace does not respect national boundaries. We know this from many different debates in which we are all engaged and we face that issue here, too.

Q345 Baroness Cohen of Pimlico: It seems to me to relate.

Professor Sadie Creese: Heavily.

Q346 Lord Strasburger: DPI—deep-pattern inspection—has already been mentioned several times today. The Home Office in its evidence sought to convince us that the shortfall between the data that they would like to collect and of the data that they are able or will be able to collect if it is enacted could be filled by DPI. My understanding of DPI is that it is a technology targeted at a single user, a single service, or whatever, and not a catch-all for the collection and retention of data. Would I be right in that?
Professor Peter Sommer: That was the point I was trying to make in my earlier rather lengthy explanation. Mostly, you use DPI as an investigative or detective tool where you know what you are looking for, whereas currently the CSP is simply told to apply the formula.

Briefly to come back to the question of the confusion in the legislation, part of the problem is that you have two distinct types of regimes. Communications data comes under the remit of the Senior Designated Officer. It is admissible and that is how it enters the courts. Content—very unusually, if we look at it worldwide—is something where a warrant is issued by the Secretary of State. It is not admissible. Although those things may be very similar technically—there is a big overlap—the fact that there is a huge gap in how they are handled by the courts is the real problem.

My own suggestion about how one reforms it is not to try to reform the definitions, which are proving increasingly difficult. Home Office civil servants have been trying to do it for several years. I suspect that you need to recast it in terms of how other aspects of RIPA work, which is to look at levels of intrusion, so you would have warrants issued depending on levels of intrusion—directed surveillance or intrusive surveillance. That seems to be a much easier route to go and do something that is easier for people to understand. That is obviously not contemplated in the Bill.

Q347 Lord Strasburger: Can I clarify what you said about DPI? Correct me if I am wrong, but I think you said that DPI is a tool for interception and that it is not a tool that will help with data.

Professor Peter Sommer: It is a tool for investigation.

Professor Ross Anderson: At present, BT has DPI capacity on about 100,000 lines; let us say 1% of the total. The other four or five big providers probably have been told to install something similar. With this capacity, in my view, you could have a regime of targeted communications data preservation, in that the software in the boxes that provide service to the 200,000 or so most suspected individuals in Britain could, right now, harvest communications data and retain it for later use. There is absolutely no reason why that cannot be done right now by GCHQ. Therefore, I argue that there is absolutely no need for this Bill and the considerable expenditure of public money attached to it at a time when we are cutting police numbers. Yes, DPI can be used to collect comms data and, yes, we have the capacity to collect industrial quantities of it at present on hundreds of thousands of households simultaneously.

Glyn Wintle: On the DPI, what needs to be understood is that software has to be tweaked or written from scratch for each new service that they wish to intercept. So every time they want to add a new service or a service changes even a minor detail, that will require programming time and that has to be applied to everything. The machine does a full intercept of everything that has been sent and then pulls out the bits that it thinks are relevant, possibly in a stupid way but we hope correctly.

Professor Sadie Creese: An additional point is that often DPI is conducted in an environment where you do not want to be detected. You do not want to stop someone communicating but you want to know what they are communicating. You are observing them. Therefore, all this processing has to happen in their real time. You have to achieve this deep-packet inspection, unless you are using it to archive, as Ross was describing; you capture it, look at it, take the bits that you want and do that without affecting the communications service of the people
involved. Therefore, it is resource heavy and costly. As my learned friend says, to do that
deconstruction, to pick out the bits that you need, you have to understand the protocol of how
it is constructed overseas. Any slight change will require effort on your part. It is not cheap
enough to do on every possible communication at will.

*Professor Peter Sommer:* I assume we are getting on to cost now.

*The Chairman:* I have questions on that, but I am conscious that we are still on the first few
questions, and my colleagues are finding this fascinating.

**Q348 Lord Jones:** Our panel is eminent and highly experienced and, self-evidently, of
integrity.

*Professor Peter Sommer:* As we are, Lord Jones.

**Q349 Lord Jones:** My colleague has used the phrase Pandora’s Box and Professor Creese’s
imprecise language. Are you as a panel, and individually, at ease with GCHQ and with the
security agencies? Do you trust them? Can we trust the agencies in which we are investing so
much faith as this legislation comes forward? What is your experience?

**Q350 The Chairman:** You are not under oath.

*Professor Peter Sommer:* I have met many people from GCHQ over the years. As individuals,
they are very often extremely congenial; technically they are very aware and very stimulating
company. At an everyday level, of course, I trust them. The dangers are as follows. First,
having a career in GCHQ is a very peculiar life. You cannot talk about a great deal of what you
are doing; and you have to go through a process of developed vetting which has to be renewed
every so often.

A lot of them are based out in Cheltenham, and that means that their world view is going to
be somewhat limited. That is not a complaint about Cheltenham in particular. I am digging
myself a hole, I can see that. It means you have a particular view and, as with others in other
intelligence agencies, and the police, you see lots of horrible things which you feel you ought
to be defending. It means that your perspective is somewhat skewed. In addition, as with a
large police force or intelligence agency, you will have groups of people who are particularly
muscular and robust and think they know best. We go back to how these people are
accountable, although that is not the subject of this session. All one has is the ISC to try to
provide some sort of control and safeguard and many of us feel that that is not quite adequate.

*The Chairman:* I will stop you there. That is a fascinating question, but I would like to hear
from other colleagues, quickly, if we may, so that we can make progress.

*Professor Ross Anderson:* I have had many dealings with GCHQ over many years. I do not
always find their technical work to be very convincing. Recently, GCHQ have been trying to
grab hold of the security research agenda and told me that that is because they cannot hire
anybody useful. They would hope that more Brits would do PhDs so that they could hire
them.

Let me tell you why GCHQ cannot get good technical staff. First, they do not pay. Somebody
with a recent PhD from our team might start at Google at $200,000 a year in California;
Cheltenham would offer them £25,000 a year, for which you cannot buy a house in
Cheltenham.
The second reason is that the structure of our Civil Service means that if you go into GCHQ with a PhD in computer science, your chance of becoming director is zero. For that, you have to go in with a degree in PPE, which is an entirely different route. People with self-respect will not go to work for a firm where there is no reasonable chance of becoming the boss. There are big issues here but they are tied in with much bigger issues to do with Civil Service reform. 

Professor Sadie Creese: In all of my dealings with GCHQ—I cannot speak for the organisation as a whole, but with everybody I have dealt with who has worked for GCHQ—I have been impressed by their level of professionalism and the way in which they go about their job. I have no criticism to make whatsoever. Speaking personally, I trust not just in that organisation but in the United Kingdom and the way in which we go about governing ourselves. Constructive work needs to be done on the Bill and on how we go about governing those mechanisms and holding organisations such as GCHQ to account and ensuring integrity, but on a personal level, I do not have an issue with trusting those organisations, no. 

Glyn Wintle: I do not think I would offer a personal view. If you were trying to model what the threats might be, you would not start with GCHQ being the biggest risk, you would probably assume that the employees of the ISP, which holds all the data, are far more likely to be a bigger risk. The fact that it has to be connected to the internet, therefore anyone can get access to it, is a risk. 

The only thing I would mention to do with GCHQ is a collection of routers that they have imported from China recently which GCHQ has approved but which security folks have recently got my hands on, audited them, and said, "These things are full of holes. How did they make it through an audit?". However, as individuals, they should not be at the top of the list to worry about.

Q351 The Chairman: Thank you very much. Interesting answers. Baroness Cohen?

Q352 Baroness Cohen of Pimlico: I am content with the answers on that. The other thing that comes to all of us is Professor Anderson’s view that, once you have traffic data, you’ve got the lot and that, therefore, access to traffic data, as opposed to use or subscriber data, ought to be in some way especially protected and more constrained. I think that his view is that the pattern of whom you communicate with and in what order gives away a great deal. Can you elaborate on what you would like to do about this in the Bill?

Professor Ross Anderson: Traffic data is coming to mean more and more as people use more and more services for different things. I am uneasy. We have to control surveillance somehow; we have to keep Britain as a society where the Government can watch anyone but cannot watch everyone. There have to be some kind of limits, be it rights limits, definitional limits or whatever. The existing definition between content and traffic data is not particularly robust and it is shifting all the time. If this is the way forward—I am not sure of that and I would personally be in favour of changing the regime so that intercept were available in evidence, as I said in my submission. But if we are to go down the route of restricting communications data we should be explicit about what we mean. If we mean call data records, that should be spelt out on the face of the Bill rather than leaving it to a future Home Secretary to decide: “Let’s by secret notice extend the definition of ‘communications data’ so that it includes your Google calendar”.
A calendar tells you who met whom when and that is traffic data, is it not? That is the traffic data as reported by a private eye following someone around and saying that he met him at such and such a time. If you were an investigator, would it not be convenient to press a button and get the calendar data for everyone who is working for a bank that you are investigating, if you are at the FSA? You can see the temptation. It is the job of Parliament now to decide whether, in the future, we will allow an official or a Home Secretary to press a button which says, “Give me the calendar data of everyone in the City and let’s investigate insider trading by seeing exactly which banker met which banker when, last year”. Is that traffic data? That is the sort of thing you have to think about now.

Q353 Baroness Cohen of Pimlico: Do you believe that the definition of communications data should extend to web activity? This is a kind of side branch.

Professor Ross Anderson: This is the fight that we had in Parliament in 2000 as the RIP Bill was going through. The Home Office thought that if you went to search for a pregnancy test online, the URL which the police should be able to get as comms data would be “Google.com/query=pregnancy+test”. NGOs managed to persuade Parliament that this was a step too far and instead that it should identify only the fact that someone had gone to Google to do a search but not what the intent of the search had been. In other words, the intent of the search should be treated as content. This question will come up again and again unless you make the definitions explicit. It will come up every time someone invents a new service, a new online context which is easier to use.

Professor Peter Sommer: It depends what you put into the log. You can tell a log to collect relatively small amounts of information or huge amounts of information. I understand why you are putting the question but unless you know the remit of the log and what is actually being collected, you cannot answer the question.

Glyn Wintle: One of the things that I found when reading the Bill was that quite frequently I thought that the person writing the Bill had thought of one particular circumstance and had then tried to write a generic version, and that does not work.

Q354 The Chairman: Professor Anderson, would I be right in saying that in 2000 you were generally content with RIPA and that the definitions of traffic, user and content were about right? Are you now suggesting that even if we did not have this draft Bill, RIPA is no longer fit for purpose and should be rewritten?

Professor Ross Anderson: We took the view at the time that RIPA was a bad Bill and we had to marshal all the available lobbying resources that we could, in the press, in the House of Lords and elsewhere, to make the best that we could of a bad job. If we were to redesign an intelligence and surveillance control regime with a clean sheet of paper, of course we would tear it up. In particular, I would like the UK to be like almost every other civilised country in having judges giving warrants for surveillance that would then include access to content. The fact that the content as well as the traffic data were available would enable more criminals to be convicted and it would also enable innocent people to be acquitted. The fact that that would all be out in the open would mean that the mechanisms of surveillance would be very much more transparent and we would not have all the uncertainty and cynicism that surrounds the interception commissioner and his colleagues.
Q355 The Chairman: If you were rewriting that part of RIPA at the moment, would you base it on Professor Sommer’s view that there should be new categories based on levels of intrusion? Merely knowing my name, address and mobile phone number might be a lower level; knowing everywhere I have been in the past five minutes when my phone is acting as a tracker may be at a higher level. Can you make up a sensible policy on that?

Professor Ross Anderson: I think we possibly could. Now that we have seen how RIPA is used in practice, we have seen that the great majority of inquiries are simply for reverse directory lookup: somebody has a mobile phone number of a suspect and they want to put a name and address to that. That is much less serious than digitally following somebody around for a week, which in turn is less serious than listening to all their phone calls and observing all their web activity for a month.

How do you set up categories like that? I am attracted to the idea that this is a task for the judiciary. As a general principle in technology policy, those countries that let the judiciary tweak the rules have a better time of it because there is a shorter time constant: the judiciary can respond within two, three or four years to a change in technological circumstances, whereas Parliaments, as you know, have very busy agendas, and not every Parliament manages to turn its attention to these questions, so you have to wait 10 years for Parliament to get round to thinking about them.

Q356 The Chairman: Yes, but we cannot give the judiciary a blank page; we have to give it guidelines of some sort.

Professor Ross Anderson: I agree entirely.

Professor Peter Sommer: An alternative route would be to task the Law Commission with the exercise. It is obviously made up of lawyers, but it understands how to make practical law. I am sure everyone here is familiar with how it works. It will carry out informal consultations, produce a Green Paper with proposals and finally a White Paper, which might work. You are shaking your head, Lord Chairman.

Q357 The Chairman: Yes, because by that time, Apple will be on iPhone 15, rather than iPhone 5.

Professor Peter Sommer: Well, a royal commission might take even longer.

Q358 The Chairman: I must move on to other colleagues. This committee has the task of looking at the draft Bill and maybe coming up with better suggestions if we think we have any. I am afraid that we do not have the luxury of leaving it all to the judges or the Law Commission. Lord Strasburger.

Q359 Lord Strasburger: Under the previous Government, Parliament rejected the concept of a large central database of retained data. If we look at the filter proposed in this Bill, does that effectively create a large database, albeit distributed among the CSPs?

Professor Ross Anderson: There are a couple of aspects to this. First, nowadays, when you compute on big data it is essentially a distributed computation. If you do a Google search there may be 10,000 machines involved in answering your query. Similarly, if GCHQ wants to make a search engine for comms data in the way that Google is a search engine for stuff, there are two ways to do it. You can either have thousands of machines sitting in Cheltenham that
have everybody’s call data records, mobile phone locations, web browsing histories and so on, and you can do the search there, or you can have these machines distributed among the CSPs, which generate and curate that data anyway, and you can create a mechanism whereby a query is sent out and the answers are brought back in.

At a fundamental level, there is not a big difference. At an operational level, there can be big differences in terms of cost and control. In terms of policy, there can be a huge difference, because if you are permitting queries to be made of hundreds of CSPs in parallel on an automated basis, that means that the CSPs themselves are no longer in a position to take a view as to whether a particular request is proportionate or necessary. I expect you will hear more about this from Google and Facebook. If you are an international firm, there are very grave difficulties indeed with giving automated access to your systems, without a human in the loop, to somebody who is going to pull together arbitrary data without justification and compute and produce an output for some other party to which you are not privy and the legality of which you cannot assess. The idea of a distributed database is in some sense the way to do it from an engineering point of view, but from a policy point of view it is difficult.

Q360 Lord Strasburger: Are you saying that it introduces risk?

Professor Ross Anderson: It introduces an almost complete lack of accountability. It creates an enormous difficulty for CSPs that hand over the data if they have to account to anybody outside the jurisdiction. In the case of BT and TalkTalk, that may not be an issue. Parliament may pass a law saying, “You cannot sue BT”, and BT may say, “Thank you very much” and hand over the data. But perhaps Facebook is not in such a lucky position.

Professor Peter Sommer: In fact, if you look at the detailed legislation and the way in which things are supposed to work with any intermediate data that is held, you have this rather curious request-filter entity. There are generic problems with it. First, it seems to operate under the authority of the Home Secretary—the same person who issues interception warrants. It is completely unclear how you will be able to set up an independent entity and staff it with people who will have any sort of career. The legislation says that any intermediate material—stuff that is collected from individual CSPs in order to produce a result for the person who is making the request—is supposed to be deleted after use. On the face of it, unless they are disobeying the law as it currently stands and unless the interception commissioner lacks the skills and resources to carry out inquiries, the centralised database could not exist in this particular form. That is the way I read it. My own reading is that all the stuff in Sections 14 to 16 is there to get over the problem that we talked about: namely, the separate regimes for communications data and content, and how it is critical that the police do not get, on the basis of a communications data request, access to content—because once you get to court, that is the route to abuse of process arguments. That is the way I interpret it.

Professor Sadie Creese: I perceive there to be two main sources of increased risk if the Bill were to move forward. First, as Ross pointed out, you may be increasing business risk to communications service providers on a number of levels. They will have to understand the regulatory and legal implications of engaging with this regulation. If they work on an international stage and keep copies of their data in warehouses on different soils et cetera, and if there are obligations to remove this stuff after a certain time period or once they are given notice to remove it, destroy it or put it out of reach, that will be very hard to achieve, technically—and to know that they have done it. If you are Google or somebody offering
back-up resilience measures that involve data storage off UK soil and all over the globe, 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. So risk will be introduced at the business level to communications service providers. No doubt you will explore that with them. Secondly, there is the issue of the privacy risk to individuals. If you are operating a distributed system, which makes sense on many levels, you have to understand that by obliging increased amounts of personal information to be stored at all of these different sites, you are potentially exposing people to risk. Because more is being kept, if the communications service provider suffers some kind of attack or is vulnerable in some way, there may be collateral damage. Equally, as this stuff is moving around as you operate a distributed system, as you pull it back into a central store, hopefully you will have your filters right and you may be less concerned about the privacy issues surrounding some of the individuals in whom you are interested. Even so, you have to recognise that as these things are in transmission and being moved around, you are potentially opening them up to risk. So there are two key areas where you may be increasing risk. You have to assess that.

Q361 Lord Strasburger: Are you saying that if the data were actually distributed among various organisations and various locations, the overall security is only as good as the security at the weakest site?

Professor Peter Sommer: Clause 16 covers the duties in connection with the operation of filtering arrangements. That is laying down what is expected, including records that have to be kept to satisfy the requirements of the interception commissioner and of the Secretary of State. Some of the points Ross makes are completely valid, but I do not think that they occur at the filtering request. The problem is much more that individual police forces collect whole lots of communications data for a variety of purposes and hold on to them because, you never know, they might be useful and then start running searches afterwards. The surveillance commissioner has commented on the extent to which the police are rather prone to holding on to records just because they happen to have them and because the cost of storage is not great.

Those are the risks that you start running, rather than with this specific entity, which I think is extremely baroque and, as I said, I think is solely to try to protect the police from inadvertently receiving content, leading to problems later on.

Glyn Wintle: It is definitely from a logical point of view, if you draw it on a diagram of any kind, one database. It happens to be distributed physically, but that is not overly relevant from the users’ point of view. I was quite surprised that the Home Office did not talk about the cost of destroying data when they talked 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, especially in the volumes that they will be dealing with. Securing this data, likewise, is going to be an interesting problem. 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. Unfortunately, you may not be able to solve that problem, because even if you store the data
centrally, you will still have to collect it at all those points and then send it, so if there is a failure at one of those points that could be quite bad.

**Q362 Stephen Mosley:** There are obligations in Clauses 3 to 8 on communication service providers to maintain the security and integrity of the data. Do you think that the clauses are adequate to protect privacy both ways?

**Professor Sadie Creese:** I do not think there is enough detail for anybody to make a judgment. There is no detail on what you mean by security and what processes will be put in place. Is it against a certain standard; who will check that for you? It is hard to say. There is obviously an intention and a recognition that there are those issues, but there is no detail beyond that to comment on.

**Professor Ross Anderson:** There is an issue here that concerns some of us, which is that if the system is used substantially for intelligence purposes rather than just policing, the history of what has been looked at will be classified at least as secret. This means if you set up a CSP where none of your members of staff are eligible to apply for security clearance or where they refuse for religious or other reasons to do so, you may end up being forced to outsource your surveillance function to one of the usual suspects—BT, Serco, Hewlett Packard or whoever—and given the way in which such markets work, I would expect that the large number of small CSPs that you see springing up in east London, most of whose founders' fathers were not born in Britain, will in fact be compelled to use the surveillance services of one or two large facilities management firms. That is how these things tend to work out. In that case, you have to ask yourself: what is the brake on innovation, what is the cost imposed on new start-ups and does the UK becoming less attractive place to set up a communications service business?

**Professor Peter Sommer:** Sadie captured it in her response. These are very generic aims. There is the role of the Information Commissioner in scrutinising it, but what sort of facilities and abilities will he have? Will he be able to carry out no-notice investigations to see what is going on? We have no way of knowing whether they will be effective at all.

**Q363 Stephen Mosley:** Those were the questions I was going to ask later.

**Q364 Lord Strasburger:** Mr Wintle, you seem to be saying, logically, that the more computers you have to attempt to break into, the greater the probability that you will succeed?

**Glyn Wintle:** The more computers, the more organisations, the more approaches, the more different ways of doing it there are, yes. If you have 10 people in charge of something they might lose it; if you have 100 people, and it is valuable, someone at some point in time is guaranteed to be tempted.

**Q365 Lord Strasburger:** Some ISPs might prefer the filtering to take place once the data has been collected centrally. Do you have a view on that?

**Glyn Wintle:** I think the guys installing backhoe cables would love this idea. You would have to double the amount of cabling provided in the UK.

**Q366 Lord Strasburger:** Can you explain that?

**Professor Peter Sommer:** I do not think it is that. I think this is the thing that was unacceptable to the public at large in 2009 when it was floated. There is no doubt that if you are looking for a purely technical solution, you do it all centrally and you ask GCHQ to do it.
If you are saying that you want to have proper controls and transparency, then the route described in the Bill is probably the way to go.

**Q367 Lord Strasburger:** We may have touched on this already, but what are your views on the power for the Secretary of State to transfer her functions in respect of filtering to a designated public authority? Would that create a more arm’s-length approach or are there certain authorities that you would consider particularly suitable for that role?

**Professor Peter Sommer:** I think it is a completely bizarre suggestion that she should be doing it because the same person who is issuing the interception warrants would, if anything goes wrong, have to be politically accountable to Parliament. It has to be much more arm’s length. The real problem about it is that if you are looking for a purely technical solution and a technical function, you would give it to GCHQ, but I do not think that that would be politically acceptable. Once you do that you would have to say: “What does this entity look like?”. People who staff it have to know their law, know their technology and they have to understand how police investigations work; they have to persuade the public at large that they are acting independently. Where do you find these people? What sort of career path will they have? I cannot see it functioning at any sort of level. You say that you will have some good ex-cybercops there, but the worry then is that they will just be too friendly with the people to whom they are talking, day by day, and will not be sufficiently independent. The only justification for this is what we keep coming back to: the desire to protect the police from inadvertently getting access to content. That is the only purpose of it. Otherwise, in the way in which it appears here, it is a completely unworked-out idea.

**Professor Ross Anderson:** As already said, I am not convinced of the need for new centralised facilities, but if needs must, I would prefer such centralised facilities to be under police control, perhaps under the control of the Met or, if absolutely necessary, under the new National Crime Agency—although its predecessor, SOCA, was not particularly competent—rather than under the control of GCHQ. If we are to establish a regime of domestic surveillance, it should be something like the FBI rather than something like the NSA. The sort of reflexes that are perfectly proper in GCHQ when your mission is to tap Chairman Mao’s telephone, by hook or by crook, are not really appropriate in a society at peace and with a very low crime rate.

**Professor Sadie Creese:** My learned friends have made excellent points. But if you want a truly arm’s-length body, you probably would not want an organisation that would be seen as operationally benefiting from the decision to issue permissions to do such things. I think you have some very sensible suggestions on the table but you could go further than that.

**Q368 Mr Brown:** On the role of the Interception Commissioner as the safeguard for the public, are you saying that he should report to a Secretary of State who is not the Home Secretary, who of course has charge of issuing the warrants?

**Professor Peter Sommer:** I think several points may be getting elided. The Interception Commissioner reports to the Prime Minister. He does an open report and a closed report. What we were talking about before was how this filtering entity would operate, how it would be funded and to whom it would report, so these are separate points.

**Q369 Mr Brown:** To whom should it report?
Professor Peter Sommer: Since I do not think it is a good idea at all, I am not sure there is any point in asking me that. I just think it is a futile idea. If you think it is a futile idea, you no longer care where it reports to.

Q370 The Chairman: Professor Anderson was suggesting that since the police have 98% of the requests, they would be a more acceptable public body to be in charge rather than GCHQ. Would most of the panel go along with that?
Mr Brown: The point is, how is that a safeguard?
Professor Ross Anderson: There is an issue among techies about the credibility of the current commissioner. For example, we wrote to the Interception Commissioner questioning whether the arithmetic in his recent report added up. I am happy to share a copy of the letter with the committee. We definitely need a little bit more quality control on the technical side of the existing supervisory arrangements.

Q371 Mr Brown: What would your ideal safeguards be?
Professor Ross Anderson: If interception were done as it is in the Netherlands, for example, where it is used absolutely routinely in serious crime cases, there is not really a safeguard issue because wiretapping is just another thing that the police do, like having cars and helicopters. Everybody understands it because it routinely comes through the courts and is subjected to testing by advocates cross-examining witnesses and calling technical witnesses. The fact that it becomes an everyday thing means that you no longer have to invent special ritual magic to reassure people.
Professor Peter Sommer: I entirely agree with that. The normal court process of disclosure and testing of evidence should answer a lot of the issues.
Glyn Wintle: My technical answer would be: do not collect a database of all this communications data for everybody in the entire country. Data you do not collect you cannot lose. By collecting it, you are creating the problem in the first place. If you have another way of solving it, please go that way first.

Q372 Lord Strasburger: Still on the filter, there will be no paper trail—
Professor Peter Sommer: Yes, there will. I saw the draft question. The intention is that there will be. It may not be there yet, but ACPO has a data communications group which is trying to design one at the moment. It is by no means complete but it knows that it has to do it. The idea is that there will be a paper trail.
Professor Ross Anderson: There will be a problem if people try to rely on the output of the filter in evidence. If the output of the filter is used only to tell the police, “Knock on the door of 13 Acacia Avenue and you might find some cocaine in the garage”, then the cocaine is the substantial evidence. If, on the other hand, the filter is used to argue in court that, “Mr A made 127 of his 387 communications over the past year with Mr B”, the defence might want access to the system so that it can say, “Actually, Mr A only made 68 out of a total 4,000 communications with Mr B and therefore this is wrong”. When you drive an engine like Google, the numerical answers you get can depend very critically on the exact phrasing of the queries you make. Once you start bringing filter-type evidence before courts, if it is ever going to be used in evidence at all, there are great difficulties about the testability of that evidence.
unless you give defence lawyers and their experts access to the machinery to kick the tyres and play with it.

Q373 Lord Strasburger: As always, it is about how you ask the question.
Professor Ross Anderson: No doubt people will become skilled at asking the questions for which they already know the answers. Over time, defence lawyers will get fed up with this and it will all go to Strasbourg and blow up.

Q374 Stephen Mosley: In previous evidence we heard that the filter would be there only for more complex cases: that often police would be able to make requests under the Communications Data Bill straight to CSPs for a lot of minor things, but for more complicated things involving multiple CSPs, a filter would be used. Would there not be some advantage in forcing all requests through a filter? You would be able to put security authentication, logging et cetera on the filter so that you would know exactly what requests had been put in because they could not go through any other avenues.
Professor Peter Sommer: You have already got, with CSPs, the SPOC system—the single point of contact. The police, or a police agency, have a single point of contact, and the CSP has its SPOC. That gives clarity. If it is a simple request, why does it have to go through an additional filter? A lot of requests will continue to be extremely simple. I would not have thought there would be a need for that at all. The SPOC system and the training that people get are designed to limit the problem of individual police officers asking ill educated questions of techies who happen to answer the phone in a CSP at a particular point. So I am not sure that your suggestion would work, Mr Moseley.
The Chairman: I will skip my question for the moment.

Q375 Lord Faulks: I will ask about impairing innovation. Professor Anderson, you discussed this in your report. If I understood it correctly, there is a danger that the Bill might effectively discriminate against smaller CSPs as opposed to an organisation such as BT, because they will be required to provide law-enforcement provisions. Is this going to stifle innovation, despite the fact that the costs are supposed to be met? Is this going to operate unfairly? What do other members of the panel think?
Glyn Wintle: One thing that I noticed during previous evidence sessions was that we keep thinking of a CSP as a telephone provider or an ISP, but it can be a service provider as well. The term covers multiple people. One of the problems you will run into quite rapidly is that if the Government are going to cover the costs, small web firms will not understand how the process will work. I would be very surprised if they recover their costs correctly. If they do, you will get gouged horribly. If you go to any software programmer and ask how long it will take to do this thing—which was not designed into the original process anyway—he will give you an answer and it will be wrong. It may be over or under, but I guarantee that it will not be correct. That will be in the paperwork but it will not be the actual cost. So one way the firm gets crucified and the other way it makes a nice little profit. Either way, there will be an impact.
Professor Sadie Creese: It is very unclear in the Bill exactly what is meant by “covering costs”. Is that the cost of a piece of equipment—of the technology? Is it the cost of your technical team’s time as you train them up? Is it the cost of your fees as a business in consulting your
lawyers on your obligations and new business risks? All these are costs—and by the way, they are not just one-stop costs. This is not just capital expenditure but an ongoing system that will need to be maintained. Fingers crossed that it never happens to you as a CSP, but you may be engaged with the system as your business changes and you change services and the software that you use to deliver them. The system will have to be upgraded, and that will not happen without some involvement from you as an organisation. These costs will exist over time. It is not clear in the Bill what is meant by costs, and whether all of them will be covered. I can imagine that it may well be offputting to a small business. We have to remember that many small businesses are involved, particularly in the cloud and apps sector, which are effectively selling on other people’s cloud services. These are not just big organisations that people buy from: there are many small organisations in the supply chain that buy white-label goods from other service providers. They will have obligations in the context of the Bill that may be offputting to them. I mentioned that many of them are not even aware of the draft Bill and the implications that it may have for their business.

Q376 Lord Faulks: I suppose that some organisations might decide that they will risk it, while others will say, “We need to cover all this” and will spend the money.

Professor Sadie Creese: Yes, it will depend on how they govern themselves—on whether they have a board, on whether the board takes legal counsel, or on what their financial director says about it. How the decisions are made will depend on that. Ross’s point is very valid. The language used in the current draft Bill is not explicit about who we mean when we say “CSP”, what we mean by “telecommunications”, what we mean by the kinds of data and services that will be impacted by the Bill, and what we mean by the costs that can be recovered. It will be very hard for people to understand the nature of the risks they may or may not be taking.

Glyn Wintle: Going back, there are also liability issues all over the house. If I change my systems and, unbeknownst to me, this breaks part of the system and I only find out about it a week later when a request comes in, and I have not logged things for a week, how much money will this cost me? Am I going to face jail time? I hope not—but am I going to face financial costs? Once again, this will act as a big impediment to me changing any part of my system once I have installed it. I would have to go back and ask you for more money to change a system that I have already paid for.

Lord Faulks: You would have to take out an insurance policy of some sort.

Professor Peter Sommer: An insurer will give you a policy for a risk only when he can calculate the odds. Speaking as someone who has worked in the insurance industry, I can say that no underwriter would be interested.

Professor Ross Anderson: There is also a potential downside for a kind of innovator that policymakers sometimes ignore: the small, community-based service. Three weeks ago I was on holiday in Skye and was able to continue doing e-mails because the lady who owned our B and B had had the get up and go to organise 20 local crofts to chip in for a satellite link. There is a surprisingly large acreage of the United Kingdom where decent internet service provision may depend in the long term on such community-based ISPs. The biggest problem they have is BT trying to stop them at every turn and looking for yet another regulatory argument to explain why they should put up with grotty old copper wire. I am mildly concerned, as are some people in Scotland, that the Bill might provide BT with yet another argument for why people on Skye should put up with 56k.
**Professor Sadie Creese:** Perhaps I may come back one last time: I apologise. I imagine that some people may respond to the question by saying, “Well, we are not interested in small organisations. The Bill is only meant for large organisations such as BT—people we can get to know and trust and who are willing to make the investment with us”. What I would put to them if I were asking them questions is: if that is true and it becomes known, and if I were into nefarious activities, I know who I would use as my communications service provider.

**Baroness Cohen of Pimlico:** I would go to Skye.

**Q377 The Chairman:** Al-Qaeda will be moving to Stornoway. Sorry, wrong island—to Skye. I will return to the question that I was going to ask before Lord Faulks came in. Professor Sommer, you said in your written submission that the bad guys could change their patterns of communication in ways that it would be difficult to detect. Clearly, using some small ISPs that have not signed up to the Home Office agreement would be one way. Are there others? What did you mean in your written evidence?

**Professor Peter Sommer:** One is always hesitant to give advice to bad guys in public, but I do not see a way round it, and all the techniques I will talk about are extremely well known. The first route is that you pay cash for a data SIM. There will be no easy audit trail to your activity. The second is to go along to an internet café. The third route would be to look for one of the large number of internet access points that are still unencrypted and to hijack it. A fourth route, slightly less well known though I currently have an instruction as an expert witness involving just such an eventuality, is where people use a web-based e-mail service. Everyone in the conspiracy shares the same credentials. The e-mail is never saved other than as a draft, but each person is able to go along to a particular web service and access it. A fifth route is to go along and use a regular web publishing service. We all get them for free with our internet service provider. You have hidden pages that are not visible by direct-linking from the front. You have a web page that is ostensibly about characters in “Coronation Street”, but if you know the direct page reference will tell you, “Let the bomb off tomorrow, and here is the plan of how to do it”. These are all routes that are extremely easy. They involve no particular skill. Once you have some skill, there are even more routes.

**Q378 The Chairman:** Putting yourself in the shoes of the good guys, how do you counteract that? How do you detect it?

**Professor Peter Sommer:** Well, if we look at the data SIM scenario, we say everybody who buys a SIM has to do so via a bank account and has to provide credentials. On the internet café basis, you have to say to the café owner that they have to demand to see a passport or two or three identification letters—I can see you are smiling; these things are ridiculous. The fact that there are all these easy gaps is important. In a sense the question you are asking is: how do we prevent burglars wearing gloves when they go about their activities? The answer is that you do not but that tells you to switch your investigative activity into areas where you are more likely to get worthwhile evidence.

**Professor Ross Anderson:** I agree, as a sort of glove manufacturer. One of my post-docs is one of the maintainers of Tor, an anonymous communication service, which is funded ultimately by the US Government through various bodies. The view taken by the State Department and others is that there is net social benefit in providing privacy to those who need it. Sure, anonymous communications networks are occasionally used by bad guys. They are also used...
by millions of people worldwide in places like China and Iran to surf the real internet rather than the internet that their Governments would rather they see. Again, it is down to Parliament, the US Congress or whoever to make these high-level trade-offs. I will say this again: this is a country at peace; it faces no existential threats and has about the lowest crime rates that have ever been recorded anywhere. In these circumstances, is it appropriate to ban the sale of gloves—or their digital equivalent? Once it is phrased in those terms, I think the answer is evident.

Lord Armstrong of Ilminster: Turning to the provision in the Bill that seeks to apply to all companies providing communications services in the UK, including overseas providers, the Home Office seems to be fairly relaxed about relations with overseas providers. How realistic is it to expect overseas providers to respond to requests to store and release communications data in accordance with British law?

Professor Peter Sommer: I assume you will have the opportunity to talk to those people and they will give you their answer. When I and other people have spoken to them, they have said, first, if they are based in the United States they have to obey United States law. Secondly, they have to think about their own customers. If their customers get the perception that there is what they regard as too easy a relationship with law enforcement—in other words, they are not exercising their own judgment—that is commercially to their disadvantage. Thirdly, any arrangements that such a company might make with, say, the UK authorities might be regarded as setting a precedent for arrangements it would have to make with other countries. I come back to the issue of lack of judicial authorisation for these things. If you are going to say to Google or Facebook, “Do a deal with the United Kingdom but by the way the authorisations are done by a politician or a senior police officer”, and that gets translated into a conversation they are going to have with some rather less benign country, that is not a precedent they would want to be involved in. You will get an opportunity to hear from them shortly, I hope.

Professor Ross Anderson: There is an issue here from the point of view of the system I mentioned. You will have a chance to talk to the Tor Foundation in due course, but it is basically a US body that provides anonymous communications worldwide as a public good backed by US public funds. If the Bill went through as it is, the Home Secretary would have the power to serve me with a secret order, which I could not then disclose to our customers in the Tor Foundation, ordering me to put a back door in the software, for example, to keep logs, encrypt these and send them off to GCHQ. A very likely result of that would be the research grant being terminated; the University of Cambridge would be £50,000 a year worse off and we would no longer be able to contribute to this multinational humanitarian enterprise.

Q379 Lord Armstrong of Ilminster: If we required international companies to keep more data on their UK communications, would there be a problem about access to that for their own Governments? If it was an American company, would the US Government expect to get access to it all?

Professor Ross Anderson: The US Government would expect to get access to anything that is retained if it produces an FBI national security letter. But people would also be concerned if Google or Facebook were ordered to keep more data in respect of all UK persons—anybody identified as being a UK national or resident, or former resident, or somebody who opened their laptop once when they were at Heathrow—then all such UK persons would become in a
sense tainted, in that if such people communicated, for example, with Chinese dissidents, those communications to and from dissidents would have to be stored for longer than would otherwise be the case. So there are all sorts of secondary and tertiary knock-on effects if UK customers become bad customers to have from the privacy point of view. I do not think anybody has started trying to think through what the effects of that might be.

Professor Peter Sommer: There is also a lacuna that I think you are identifying in your question, Lord Armstrong, which is you only have jurisdiction over data that is held on your territory, as opposed to the alternative interpretation that if you have access to it—in other words, you have a terminal in your country that enables you to get access to stuff overseas—does that not give you jurisdiction anyway? There have already been cases not involving RIPA but involving obscene publications, for example, about how far the courts had jurisdiction. I know because I was the expert in that case; it went to the Court of Appeal.

Q380 Lord Armstrong of Ilminster: Are the mutual legal assistance treaties relevant in all this? Will there be overseas providers who will only operate subject to those treaties?

Professor Peter Sommer: That is a question that would be best put to the police, who have operational experience. I have indirect experience because I have been involved in a police investigation, or I have been a defence expert and I have seen the activity. If you are going the full, formal MLAT route, it can be very prolonged, even with the United States—and the United States and the UK probably have the best relationship; there is typically an attaché in Grosvenor Square who will handle all these requests as expeditiously as possible. Normally, what seems to happen in investigations is that informally the investigating officers in different countries happen to know each other because they have met at conferences or done training together or whatever. They then ring each other up and say, “Interesting situation, we’ll sort the paperwork out later, wonder if you could help us out”. Once you start going the MLAT route, it can be very laboured.

I was involved in a case about three years ago. I will actually name the party because I think it has changed its policy now but at one stage Yahoo was being extremely difficult about dealing with UK law enforcement. In fact, UK police officers went to collect evidence from Yahoo. Yahoo would not talk to them but said it would talk to the FBI. So the UK police officers talked to the FBI, who then talked to Yahoo. The FBI officers came out of the room and gave the UK police officers what they wanted. I think things have got a bit better than that, but it illustrates what can happen.

Q381 Mr Brown: How is that a safeguard if you are on the receiving end of all that?

Professor Peter Sommer: It is not a safeguard.

Professor Ross Anderson: American law is the safeguard, it would say.

Q382 The Chairman: Professor Anderson and Professor Sommer, I know that you are not experts on America but one of your papers mentioned the NSA and that, after the Twin Towers, the President ordered the NSA to trawl everything they could and it was not until about 2007 that their trawling was put on a slightly more legal basis. If the Bill goes through and the British Government ask ISPs based in the States—Facebook and Google—to store a lot of material on British citizens, bits of which the United Kingdom may very well want to access with a proper intercept warrant and so on, once all the raw bits of data are on American servers, do the American Government have the right to take the whole shooting match
without having to go through a legal process to identify the bad guy as Professor Sommer or whoever?

**Professor Ross Anderson:** The current routine with FBI national security letters means that, in effect, the FBI can seize any material that is on US soil and it does so entirely secretly. Until very recently it was said that you could not even talk to your lawyer. There was a chap who owned a small ISP in New York who challenged that. He talked to his lawyer. He was the Dole in ACLU & Dole v the Department of Justice. Only very recently was that resolved and now you have the right to speak to a lawyer if you have a national security letter served on you. However, essentially there is no safeguard for British data on American soil. Given that Facebook, for example, keeps all its data on American soil, if the UK Government orders Facebook to keep data on UK citizens which they otherwise would not keep, that is data that is being made available to the FBI, like it or not.

**Q383 The Chairman:** And they can use it any way they like without having to ask the Home Secretary here, “Can we please check on Anderson, this dodgy character from Skye?”

**Professor Ross Anderson:** Who is this Home Secretary?

**Professor Sadie Creese:** That is my understanding about the arrangements in the US at the moment too. We must not forget that the scope of the Bill will not just affect stuff that happens in the UK and the US but it will be potentially global. Many of the markets that are opening up are in South America. The game is over in India, as everything has moved on now. Whole supply chains exist behind these communication service providers and they are stacking up because they have to manage their peaks and troughs in demand, so they build supply chains behind them and that affects where data resides globally and where you get your services. You have highlighted in the past few minutes the arrangements with the US and the legal position there, but of course we are led to believe that we have a very special relationship with the US—I am not a lawyer—and one can only imagine what the arrangements will be like globally.

I want to bring this back to the point that I made earlier, that one of the areas where you are potentially increasing risk is around personal privacy and enterprise privacy. You are potentially requiring people to store more than they would otherwise do. If that storing activity takes place outside UK sovereign soil, our ability to govern that, to protect it, to oversee its integrity and security and so on and to prevent foreign Governments from having access to that for their own purposes creates a challenge. There are probably many foreign Governments who would be interested in a lot of commercial assets that are placed in some of these environments. That challenge relates to the issue of risk.

**Q384 The Chairman:** That leads nicely into the questions that I anticipate Mr Mosley may wish to ask you.

**Q385 Stephen Mosley:** A lot of these points about the database were covered earlier. On the last point, I would like to clarify something in my mind. When you have an overseas provider, like Yahoo, or whoever, would the British Government ask them to collect all data or would they ask them to collect only data coming from people in the UK? In that case, how would they differentiate?
**Professor Ross Anderson:** That is one of the most difficult problems. Suppose, for example, I am a wicked foreign intelligence service in South Sudan and I want to find out what you are up to and suppose that Google has mechanisms, following entreaties from the British Government, which will allow Governments to access the data of anyone on their territory, and suppose that that data is held in Gmail, then I would follow you around using a well known law enforcement device called an IMSI catcher. That is something that you can buy for €100,000 or so from Rohde & Schwarz, it is a standard piece of police kit. It is basically a false mobile phone base station, which you carry around in your car when you follow a suspect so that all his mobile phone calls are relayed through the police car and through the police station and therefore can be listened to, rather than simply going off encrypted to the nearest cell tower. If I am a member of the South Sudan secret service here in London and I have an IMSI catcher in my car and I drive around behind you while you are using your laptop or mobile phone or your tablet on official business, I can teleport your session so that it comes out at an IP address in Juba. Therefore I can say to Google, “Mr Mosley is currently in Juba, please give us all his Gmail”. If you are concerned about that sort of thing as a threat to the security and integrity of UK persons, as you should be—a number of Ministers at Cabinet level and below and many senior officials use Gmail because it works better than the official stuff—how do you go about creating an environment of rules, in collaboration with firms like Google and Facebook, which prevent attacks on the UK being conducted so easily with a piece of equipment that you can drive around with in a car?

**Professor Sadie Creese:** Perhaps I may build on that. We need to remember that not everybody uses a recognised social security-type identity when they are accessing services. Not all communication service provisions require you to authenticate who you are; you can sign up with an e-mail address and a name and so long as it works, you are away. One of the challenges that the intelligence and police agencies will face, as has been noted in the documentation, is how you link together these identities and make the connections across them. Of course, that is not for the Bill to define, but you quite rightly recognise that there is an issue about how you go into an organisation and require it to keep only records relating to UK citizens when the identity tokens that they use for their service users do not in any shape or form require them to have authenticated themselves as UK citizens when they signed up. This falls into that business risk pot for such organisations. How would they go about meeting your requirements if they do not know these pieces of information?

**Glyn Wintle:** As you can imagine, this gets horribly complex. We are trying to keep it very simple. We could go on for several hours on this. At the simplest, you travel to a country, you log into your web mail, so are you now subject to access requests for all of the web mail?

**Professor Sadie Creese:** I will say something constructive. You could sit back and reflect on this and say, “Okay, in such cases we can therefore not require them to store this stuff”. If the Bill applies to UK citizens and registered organisations and businesses and certain types of communication services do not keep the records required for us to identify the subset of their users that fall into those categories, then you might say, “Okay, we cannot require them to adhere to this Bill”. There are constructive ways out of this.

The panel is putting to you the fact that some real reflection needs to be made on the scope of that challenge and the value that one will get from passing this Bill in the face of such limitations.
Q386 Stephen Mosley: We have talked about people who are physically in the UK, in South Sudan or wherever. What about where they are not in the UK but are using services in the UK or even aware they are not in the UK, not using services in the UK, but it is being routed via a cable that goes through the UK? What is your view of how the legislation would affect those people?

Glyn Wintle: It has been very clear. I loved the way that it was sneaked in at the end of the Home Office’s answers. He listed a bunch of things and then trailed off at the end and said, “and communication that passes through the country”, as rapidly as he could and moved on. The Home Office has already said that any communication that passes through the country is definitely counted. Data that is already held in the country? Yes, definitely.

Professor Peter Sommer: There might be a degree of obfuscation in the legislation from the beginning when it says that it is maintaining a capability, when you really have to stretch language to believe that. Paradoxically, that is creating a political problem for the Home Office: there are so many of these things that you are properly asking about for clarification, and yet at the same time we are being asked to trust these people to look after us. It is so easy to interpret the legislation as saying that there is a loophole here and a loophole there.

Q387 The Chairman: I would like to come back to you, Professor Sommer, on the so-called 25% degradation of capacity at the end. Do you have any more points Mr Mosley.

Q388 Stephen Mosley: One last thing. It is something that I have asked previous panels. Clause 1 and the powers given in the first subsection are very wide ranging. I touched on that earlier. Do you think that they should be tightened and made more explicit?

Professor Peter Sommer: Absolutely. We are being told that it is a good idea to have framework legislation because that gives a great deal of flexibility. I understand that. Then they say, “Do not worry; there can be scrutiny; it has got to go to various bodies and, in the end, it is an affirmative resolution of Parliament, and that is the ultimate control”. You have to question that on two grounds. First, with all respect to parliamentarians in general, this is extremely tricky stuff; it is outside their normal experience and I invite members of the Committee to think about that. Secondly, if you are going to ask why this is necessary, you will want to know what are the particular reasons, but you have already heard from the police that they do not particularly want to talk about them in public because that would identify weaknesses in current surveillance capability, so that control does not really exist. That is the problem.

Q389 The Chairman: I am still interested in the international aspect and what I perceive as a potential risk to information on British subjects stored on overseas servers or mega hard drives. We have already discussed Facebook and Google in the States. Hypothetically, say Facebook or even BT finds that its servers here are overloaded or overexpensive and they set up a server farm in India. Would all information on British citizens stored on what I presume would be a cheaper server farm in India then be accessible to the Indian Government?

Professor Ross Anderson: Yes, that is how things work at present. If you have a btinternet.com email address, that is subcontracted to Yahoo, so the FBI can knock on Yahoo’s door, produce a national security letter and get your stuff. If you are concerned about that, you should lobby the new Secretary of State for Justice to push in Brussels for the new data protection
regulation to be made stricter in its safe haven provisions rather than, as his predecessor was lobbying for, it to be made toothless. There is an option open to parliamentarians there, although I suspect that it might be considered to be slightly outside the remit of this Committee by Ministers.

Professor Sadie Creese: Just reflecting on that, we have to recognise that much of the data is already stored in those parts of the world. Therefore the Bill increases risk if we are requiring them to store more than they would normally. If this stuff is already being stored in all those different parts of the world, the effect of the capital may be neutral, but it is increasing risk if we are asking them to make available more data or the same data for longer periods, and the like.

The Chairman: So in 2000, if the FBI or NSA logged on to my mobile phone, they would have got the basic stuff my little Nokia had: a few numbers and about 20 addresses. Now if they log on to my top of the range iPhone, they will get a thousand times more information because that is available. If we ask them to store more, they can access it. In your view, is there a risk that other countries in the world where there is a data farm thingy could do likewise?

Professor Sadie Creese: If the Bill puts an obligation on companies working in an international space, a global market, that results in them storing more of our personal or commercial data abroad than they would have otherwise done, then the Bill has potentially directly led to an increase in risk, yes.

Q390 Baroness Cohen of Pimlico: Were you hosted on an American server, as you would be with Yahoo, the Americans, receiving any kind of inquiry, would think, “You know, we will have a look”, and you would find yourself being extradited to an American prison before you could breathe in.

Q391 The Chairman: That is an interesting observation. We will move on to Lord Jones.

Q392 Lord Jones: With your expertise and insights and long-term experience, you give your answers but in the end they all point to a central dilemma: trust and risk. From your experience, do you believe that the Home Office, year in, year out, can face up to the pressures of British intelligence agencies? The Government are separate from this Committee. We are parliamentarians. Above all else, our duties relate to liberty and the defence of it, the citizen’s rights. That is our duty in this Committee. The Government may have some other view. It seems to me that we need a little more advice from you on how the Government can cope with the pressures. It is the liberty of the individual and it is the security of the state—the defence of the realm, if I may quote from MI5’s motto. It will never hurt a Committee like this to hear your views as to how the checks and balances may be operating.

Professor Ross Anderson: That is a big one. I suppose my view is that the intelligence agencies were perhaps rather ill advised in allowing the Bill to go forward because it has made salient many things, which, had they not been brought to public attention, people would not have bothered about. It is a hard enough job for NGOs such as FIPR, PI and Big Brother Watch and Liberty and so on to get people to pay any attention to this stuff. Were I the director of GCHQ, the last thing I would want would be for a Home Secretary to bring a Bill like this, which would get wind in an awful lot of these sails. The simple fact is that technological progress has provided an absolute cornucopia for police and intelligence agencies. Instead of simply the call data records and location history that the Lord Chairman’s phone gave away in
2000, there are now vast amounts of stuff: all the websites you have gone to, all the things you have been interested in, places you have gone past, QR codes that you have scanned. It is an absolute river of data. For the Home Office, in the midst of this plenty, to be shouting, "More, more, more!" rather than organising quietly and efficiently to make more effective use of what it has already is bizarre.

Q393 The Chairman: You say there is a cornucopia of data. I picked that up as well in Professor Sommer’s paper, that there is a huge lot more data. The Home Office tells us it has lost 25%. Square that circle, please.

Professor Peter Sommer: There are several issues here. First, in the past 12 years or so, the amount of potential digital evidence available to the police for investigation aside from communications data has become phenomenal. Hard disks have got much larger. Three-quarters of us have a personal computer. All of those are very rich sources of evidence. The suggestion that if we do not get this communications data we are in trouble really is nonsense. There are lots of alternative avenues and when you come to look at value for money you have to consider the potential costs of this particular exercise against the 20% reductions being sought by the Government for law enforcement agencies.

In terms of trust and how you manage it—your big question—I would be quite interested to hear Lord Armstrong’s views since he must have had a much better view of this than almost any of us. The impression I get is that politicians start out with very much the sort of views that you want but once you are a Home Secretary you are confronted with the possibility, supposing you do not let this bit of legislation go through, of being the politician who has to stand up in Parliament and explain that you refused the police or the spooks this sort of thing and you are terribly sorry that 52 people got murdered in the Underground by terrorists. I suspect that is the real pressure. We all have our views. I do not want to be too personal about it. A man with Charles Farr’s background is perhaps not the best person to give a completely balanced view of the risks to the Home Secretary.

Glyn Wintle: On the very non-technical but broad question you asked, there is a phrase which I shall horribly mangle: it is poor social hygiene to pass laws and build infrastructure that can then aid a police state. I think that is true, but on the more specific issue, I would be far more worried about a cock-up than some conspiracy or rogue elements. For a couple of years, I maintained a log of data losses of various NHS and other government bodies publicly acknowledged in newspapers. It worked out at a data loss every two days of between 200 and 2 million records, all personally identifiable and sensitive. The NHS seemed to be winning hands down by losing incredibly sensitive information every three days for three years running, at which point I gave up because it did not seem to make the blindest bit of difference when you pointed it out to them.

Professor Sadie Creese: How to find a way through this? Speaking personally and professionally, I have to say that the days of assuming that we exist in physical space with cyberspace going on around us are long gone and, frankly, old-fashioned. We need to embrace the current and future reality that everybody exists in cyberspace to a certain degree. When you speak to people outside of our profession as governors and security professionals—friends of mine who might be teachers or housewives and the man on the street equivalents—most people would like to see cyberspace not as a Wild West where anything goes but for there to be some notion of governance and protection. They will see that as safety and security
for themselves and their families in their working and home lives. They will accept that we have to do something about taking our current mechanisms for governing society and extending them into cyberspace.

On that basis, I would not rule out at some point—now or in future—having a Bill that recognises that the current tools of the trade are not fit to make that extension. That said, I feel that all those people would expect the law, democracy and the same levels of integrity and governance to be to be applied to that.

The issue that we face here is the same. Technology is so enabling. Not only is it the ultimate asymmetric tool for nefarious activity because it is very easy to do bad things from remote places and the cost of entry is small—you just have to buy yourself a little computer—but there is also the potential for the police and intelligence agencies, if they are acting with bad intent, with access to vast amounts of data to use that for wrongdoing. Therein lies the challenge, does it not? Gone are the days where you can rely on the natural tensions, the fact that there is limited resource so you cannot spy on every person in the country because that is not practical. Now, with the advent of modern computing and services, the art of the possible is vastly increased for both the police state and malicious people. The degree to which we are dependent on it as individuals, as a society and as a nation has increased, too.

I do not reject out of hand the notion that some modernisation is required to the way in which we do our governance, given the changes that we have witnessed in our society in engaging in cyberspace, but I do say that the current draft of the Bill does not go far enough to define what is meant by its scope, how we would go about governing such a thing and holding to account the agencies that would have access to that data.

Glyn Wintle: Just a quick follow-on. Other witnesses talked about the Bill making the internet more secure. There might be things you could do—laws you could pass or more money you could give to organisations—to secure the internet, reduce the amount of spam and all those kind of things. This Bill does not do that.

Professor Ross Anderson: Perhaps I might make a small follow-on. In June we published a report on the costs of cybercrime that had been commissioned the previous year by the Ministry of Defence. It asked what we should do to clean up the internet. We did a very thorough study and the conclusion that we came to was basically that more money should go to the police so that they could lock up more cybervillains. There are very positive things that can be done without changing legislation. It is just a question of giving police money and telling them to roll up their sleeves and get on with it.

Q394 Lord Armstrong of Ilminster: Do you think the police have the technical know-how to do this?

Professor Ross Anderson: It is beginning to get there, with the Metropolitan Police’s e-crime unit.

Professor Peter Sommer: It is extremely patchy. I see this more or less on a daily basis as an expert witness working in the courts. There are some UK police officers who are fantastically well skilled and even write programs that are used worldwide. They tend to be at the level of constable or sergeant, and their career paths are not terribly well thought through. But once you get outside that elite, skills are quite patchy. If you are looking at law enforcement, you need to look also at the capability of the Crown Prosecution Service and of the barristers who might be instructed to handle this sort of thing. The issue extends well beyond cybercrime. As
Sadie said, you can almost no longer distinguish between the cyberworld and everything else. Digital evidence is everywhere and on the whole it is pretty badly handled, other than by the elite groups.

Q395 Lord Armstrong of Ilminster: My involvement in this was some years ago. If I were looking for expertise within government on this kind of thing, I did not look to the Metropolitan Police but to GCHQ. I would not have known where else to find it, except possibly the Ministry of Defence.

Professor Peter Sommer: Do not forget that the police’s skill is in producing admissible evidence, as opposed to producing intelligence. They are quite skilled at that. The sort of thing that may be produced by an intelligence agency might never be made public. You are looking at lower levels of certainty, whereas police evidence must be testable.

Q396 Lord Faulks: Following on from that, we have a system of trial by jury. Apart from anything else, the prosecuting authorities have to be able to present the evidence in a way that 12 randomly selected people are capable of understanding. Is that a real problem?

Professor Peter Sommer: It varies considerably. It depends very much on the skill of counsel and, if I may say so, of any expert who is asked to speak to them and to find the right sort of language. We are probably going way off the subject of the Bill, but it is a matter of great interest to me. As you know, we cannot ask jurors what they think, which is a great disappointment. Frequently I find myself in court, looking at jury members and wondering how much they are taking in. On the whole, I have not had many situations where I have said, “Gosh, we had a bloody good explanation and the jury just did not get it”. It is down to skill.

Q397 The Chairman: Perhaps I might come back to what is, in my view, a crucial point. We have been told by the Home Office, we have read it in nearly every document and heard it in nearly every statement that the driver behind this Bill is that things have changed since 2000 and there is a 25% loss of data. It is vital to get that data and if this Bill goes through, Mr Farr hopes it will get up to about 85% recovery. Professor Sommer, you say in your paper, paragraphs 5 to 10, and you have said today, that there is a huge increase in the data available. This hurts my little brain. Is it that the Home Office is saying that there is a 25% drop in theory of what it could have if it had everything available, or has there been an actual 25% drop in the millions of bits of information since 2000?

Professor Peter Sommer: I do not know where the figure comes from or what the basis for calculation is, but what they are talking about is simply the communications data. We need to go back and look at what the overall agenda is. What the Home Office is saying is, somebody falls under suspicion and the police commence an investigation; they look for various types of evidence that might be around, including communications data, how people behaved in the past. CSPs are asked to store the data over a period of years is because it is collected from everyone on the basis that a tiny percentage of us might go bad and you want to know in the course of your investigation what those people have been doing before you became suspicious of them. But this is only one strand in the investigation. In addition to that, you will have witness testimony; if the people have fallen under any sort of suspicion you probably have grounds for seizing their hard disk; you have the ability to get their banking records; there is
also a huge automatic number plate recognition database. So the 25% figure simply relates to retained data—at least that is what I understand the Home Office to be saying.

**Q398 The Chairman:** Has that dropped 25%, in your opinion?

**Professor Peter Sommer:** I do not think it is a question of dropping—

**Professor Ross Anderson:** The sort of complaint one hears is this: in the old days you could get call data records about who phoned who but nowadays if you go to somebody like Facebook and say, “Please give us communications records between this wicked Professor Sommer and this wicked Professor Creese”, Facebook will simply say, “Professor Sommer logged on last night at 7 pm and logged off at 9 pm”. You then ask Facebook, “Did they send any messages? Did they poke each other? Did they write on each other’s walls? Did they tag each other’s photographs?”, and Facebook says, “Sorry, we are a respectable US company. That is content. If you want content, get the Home Secretary to sign a warrant, send it to the FBI, get them to counterstamp it and serve it on our headquarters at Menlo Park”. Whereupon the security service basically goes away in a huff because it cannot be bothered to do that. This does not relate to stuff that existed in 2000. Facebook did not exist in 2000. If Peter and Sadie were having an affair back then and you wanted to find out, you would have to follow them around physically in a car. *[Laughter.]* So the missing 25% is not anything that used to be there; it is just that instead of getting a large proportion of a small amount of data, the Home Office is getting a large but not perfect proportion of a very much larger amount of data.

**Professor Sadie Creese:** We are getting to a really very important point here. The issue I raised earlier was that in general people would like to see us properly govern cyberspace and make sure that things are updated. But we should remember that people believe that this should be pointed and there should be a justification for accessing this kind of material about people; that fundamentally in this country we have rights to privacy; we are innocent until proven guilty. I am not a lawyer, but we grow up in a spirit of Britishness and fairness, and if you talk to people in the street they will expect you not just to go around collecting everything possible because it might one day be important about people who are fundamentally innocent of any crime for the entirety of their lives, give or take a speeding ticket. This builds on the issue that Ross is raising, that realistically you have good reason to believe something. There should be appropriate checks and balances and you should go get the stuff that is relevant. I am not sure that that is exactly what this Bill is about, as currently presented.

**Glyn Wintle:** The flashcard version is that beforehand, there were 100 telephone calls and 100 are the messages sent and now there are 100 telephone calls, 100 of this, 100 of that, 100 of that, 100 of that, and 100 of that. Therefore, if you count all of that, the percentage has gone down, yes, but the total amount of data has gone up.

The slightly flippant comment tweeted to me when I was live tweeting one of these sessions was that someone said, “By that same logic, we should collect all refuse that is thrown out and keep it for a year, because it could be very useful for a police investigation”. If it were zero cost to keep all that garbage, by the same logic, you should.

**Professor Peter Sommer:** Perhaps I may say briefly how important it is in what I assume will be private sessions with law enforcers that you try to establish in your own mind what types of data they find really important, instead of talking about global percentages.

It is my strong impression, for example, that mobile phone location data, which is extremely important, is not going to be affected by any of the changes we forecast. It is my strong
impression that basic IP data will not be changed, although we are moving to a slightly different protocol.

I also urge you to probe some of the anecdotes that you are being offered about importance. Some of the anecdotes that you heard in the police evidence about the importance of communications data were, I am sure, true, but when you dig into them—I have personal knowledge of one or two of them—they are not illustrations of the need for the Bill. That stuff they already have and will continue to have.

Q399 Michael Ellis: I presume that the panel accepts that the ability of the police and the security services to keep up with advancing technology must be maintained. We are now in a very different position to where we were 30 years ago, when there were simply landline telephones. To use the analogy to which several of you referred a few minutes ago, the fact that there is a greater range of communicative ability—people use different forms of communication now, such as Facebook, the internet and the like—means that more nefarious activity is happening using those media. The police must keep up with that, must they not?

Professor Sadie Creese: I agree.

Q400 Michael Ellis: The fact that there has been a deterioration of in the region of 20% to 25%—obviously that is an approximate estimate by the security services—is 20% of a greater mass of material is not in itself relevant, is it?

Professor Ross Anderson: I think it is relevant.

Q401 Michael Ellis: May I finish for a moment, professor? Is not what is relevant the fact that 20% of the current quantity of material is being lost to the police and security services by being unable to act in the way that they used to?

Professor Peter Sommer: It is back to the glove argument, isn’t it?

Q402 Michael Ellis: No, I do not accept that it is. You were saying, Professor Anderson.

Professor Ross Anderson: The stuff that they would like to have now but do not is stuff that they never had any-way. When you probe the police, you will find that the real operational requirement of the average chief constable and further down is for better police forensics. That is an issue to which the Home Affairs Committee has turned again and again over the past 12 years. I have spoken to it twice about the issue so far. Forensics have not kept up. There have been all sorts of problems with various forensics services, contractors and regulations about forensics. Nowadays if you go and bust a street-corner drug dealer, he has two laptops, five iPhones, 10 iPods and a whole bunch of memory sticks. He has many terabytes of data. The cost involved in indexing all that stuff, making it available for the defence during trials and deciding how to use it is simply beyond the system's capacity to cope.

This is stuff that we have already and are not using. Why? Because resources are being misallocated. If the Home Office were running this thing properly, they would fix the forensics problem before dealing with this kind of blue skies stuff.

Q403 Michael Ellis: Would that not be the same as saying in 1900 that we do not have the apparatus to collect fingerprints? Is that not the argument that you are making? You have
referred to the fact that they would not have had the data that they can now get anyway and they would not have had fingerprint data 120 years ago so why bother to start collecting that? Now we can monitor nefarious activity through different forms of communication.

**Professor Peter Sommer:** You have to apply a value for money exercise at the moment. I repeat what I said earlier and what I have said in my paper: there are 20% depletions in budgets. When you start looking at the costs of this exercise and what you will get for your money, it does not look very good compared with doing digital forensics on hard disks. I declare an interest as that is how I earn quite a bit of my living, but I think it is an important issue.

**Professor Sadie Creese:** However, in fairness one cannot always access the physical equipment to do the forensics. I think it is entirely reasonable that we would periodically review our police forces’ and intelligence services’ ability to go about their jobs. We recognise that the world has changed significantly, not just in the past 30 years, but it continues to change apace and almost quicker year on year. You look at the business models, you look at the way in which people are operating and conducting their lives and business and how we govern our country with government services online and the like, and it is an incredibly important endeavour. We should try to find a way of enabling this to happen with the correct controls around it so that we can preserve people’s privacy but also enable us to pursue investigations inside these environments and not simply create a corner of cyberspace.

**Professor Peter Sommer:** You are absolutely right. We need regular reviews. The landscape changes; we need to understand the landscape and then we can make determinations. Looked at in terms of what we have to do now as regards the Bill, I suspect that this is not good value for money.

**Glyn Wintle:** If you choose to collect all this data, it is a matter of approach. It is the same argument that has been made before about installing cameras into rooms because things might occur in the rooms that we do not want to find out about. We are not saying that we should not be able to investigate things that happen through those mediums, but if your solution to the problem is to collect data on everybody in the hope that some of it involves badness, then that is very expensive and not necessarily a very good way of doing it. It has some horrible consequences.

**Professor Ross Anderson:** I suggest that you ask police witnesses from an average-sized police force. The £200 million a year over 10 years that we are talking about translates to £5 million a year so you could ask, “How would you like this £5 million a year spent, chief constable? Would you rather have a communications database or an extra helicopter and another 70 officers?”

**Q404 The Chairman:** It is a question that the Home Affairs Committee will no doubt ask.

**Q405 Lord Strasburger:** What are the costs of these proposals?

**The Chairman:** I thought we had covered that one.

**Q406 Lord Strasburger:** What are your views on the £1.8 billion estimate?

**Professor Peter Sommer:** Perhaps I might answer that quickly. They have said that they think that the internet is going to increase in size by 10 times over a period of 10 years. No sensible person could possibly make that sort of forecast; we have absolutely no idea. All they are
looking at is volume of traffic; they are not looking at complexity of traffic, which is certainly an important issue. You have also heard that the costs are not only at start-up. You have an ever-expanding requirement to increase the hardware capacity and, if you are going to do it, the software, the DPI stuff, will need constant revision as well. Although none of us can give you the actual figure, if someone were to tell you that they could rebuild the Palace of Westminster but with completely modern facilities for £2 million you would know they were talking rubbish and I think we may be in a similar situation with the forecasts from the impact assessment produced by the Home Office.

Glyn Wintle: The impact assessment said that the majority of costs would be on training. I was a bit confused on that point because I would imagine that the ongoing costs of keeping the interception side of things going will be by far the greatest costs. If the costs are equal, then their estimates will be quite a long way off.

Q407 The Chairman: Is there a danger, if the British Government say to Mark Zuckerberg, “We want you to install some fancy black boxes to record all this material”, that he will try to recover the £42 billion he has just lost by going for gold-plated black boxes and making us pay for top of the range equipment? That is a loaded question, but is it a genuine possibility?

Glyn Wintle: If I had legal liability—say I was based in America and losing data would cost me money and definitely lose me customers—why would I not go for a gold-plated solution? I may have liability issues, but liability is not even mentioned in the Bill. Either way, I am worried. If you say, “Do not worry, we will cover your liability”, my customers should be a bit upset. I would worry if I were the UK Government, as well. Once again, are you going to cover American court costs?

The Chairman: A point that has not been raised.

Q408 Stephen Mosley: There was a lot of preamble there, Professor Sommer, but at the end you said that the cost estimates were a load of rubbish. Did you mean that the cost estimates we have here are a load of rubbish?

Professor Peter Sommer: Yes. It seems to me that you have got a whole lot of issues. For example, they say that they will not cover every internet service provider. We have talked about people taking simple evasive techniques, so what exactly are you spending your money on? You do not want to spend all your money on collecting stuff from people who are of no interest; you want to collect from the evaders. If your system is going to work at all in terms of capturing material on people about whom you do not know at the moment but might want to know in future—that is the agenda—you have to have pretty near 100% coverage. That is not reflected. What I suspect will happen if this legislation goes through is that there will be an initial cost estimate and then several months later they will say, “Oh, there have been unforeseen circumstances, we will have to increase our costs if we are to meet our aims”. There will not be any proper discussion because it will all be under a security blanket. Any contracts will be commercially confidential and you will have the standard recipe for runaway UK government computer projects and runaway MoD projects, with people unclear what they are doing. One of the really big risks to the taxpayer if this thing goes through is an ever-increasing expense until eventually people realise that it is a waste of time. Most people around the table will recall one or two computer and MoD projects that followed this precise pattern.
Q409  The Chairman: I am conscious that we have gone on for rather a long time. A last question from Dr Huppert.

Q410  Dr Huppert: Just briefly, Zoe O’Connell on the Complicity blog did an interesting analysis of the current costs per request and came up with a figure of about £30 per request. Doing the figures from a police source, I made it about £170. There are some differences there. In contrast, an extra 15% of the data at the moment, at £180 million a year, comes to about £2,500 per request. Do those figures sound about right, in your experience? Is there any fundamental reason why the new data that we are getting should cost an order of magnitude or more than the old data?

Professor Ross Anderson: You have to be very careful about the difference between fixed costs and variable costs. Where fixed costs are high and variable costs are low, you can end up with some funny effects. Here you also have to worry about liberty, so it is actually a good thing that a policeman who wants my cell site location history has to hand over £600 to Vodafone to get it. I consider that to be a feature rather than a bug. If it were possible to go and spend £2 billion, £20 billion—whatever magic sum—and build a vast system of systems where the marginal cost to a policeman of getting your mobile phone location history for the past year was micro-pence and could be completely disregarded, so your mobile phone location history could be requested several times a day as part of larger and more complex searches. You would then have removed what is at present the main practical obstacle to abuse of surveillance on an absolutely industrial scale such as we saw in the former East Germany. You have to be very careful about economics, about capital cost versus marginal cost. At the moment we have marginal cost. At the moment you have Mr Google saying, “Fine, we will refer that to a lawyer and get back to you this afternoon. The lawyer’s time costs £100. Here is the invoice, plus VAT”. That is a good thing. If you make it go away, here be dragons.

Professor Peter Sommer: You also have to look at the different types of CSP and the different types of request. In the case of mobile phones, call data records plus location tends to be a very standard type of request and it can be—indeed, is—semi-automated. Your specialist adviser will be able to tell you a great deal about that at some point. If you are looking at the more complex type of inquiry, you do not know what the figures are going to be. As Ross was saying, if you are having to interpret the law and translate the law into technology, as we were discussing earlier, these simple percentage figures and these simple global figures do not assist us at all.

Q411  The Chairman: Excellent, thank you very much. Lord Armstrong, a very final question.

Q412  Lord Armstrong of Ilminster: Today’s discussion has been all in terms of the police and the intelligence and security agencies. Under RIPA, the powers to have access to this sort of data extended way beyond them to local authorities, the Gambling Commission, the Child Support Agency and so on. Do you have any views on the extent to which these powers should be granted to public authorities?

Professor Peter Sommer: That is the subject of the Protection from Freedoms Act—is that what it is called?
Q413 Lord Armstrong of Ilminster: Protection of Freedoms Act.

Professor Peter Sommer: Yes. I understand the difference. You raise a very good point, Lord Armstrong, that you can perhaps expect levels of skill and a single point of contact in the police and the intelligence agencies. One area of difficulty in extending it beyond them is the local authorities, because they also have the trading standards people, who do really quite complex investigations. The way you phrased the question I think perhaps indicated the answer.

Professor Ross Anderson: It is also important to consider civil litigation. Once evidence exists that can be used in a civil case, a High Court judge can be persuaded to grant an Anton Pillar order or a Norwich Pharmacal order or whatever. This might be thought to normally affect only litigation between large parties that can afford it, but recently there has arisen a fashion among content providers—publishers, Hollywood and so on—of suing large numbers of individual citizens for alleged copyright infringement. There will remain a worry in the minds of many people that if a communications database is constructed for use by the police, it will not be very long before Hollywood lawyers are knocking on the doors of the High Court asking for a copy. Parliament had better consider this if it is going to bring in such a law.

Professor Sadie Creese: If I may respond to that off the top of my head, without any preparation, I would personally be ill at ease with that amount of data being accessible to local authorities and the like. It is a very different matter when you are talking about fighting crime and the kinds of activities the intelligence agencies engage in. I would welcome a wider debate on that. If we were to pursue this kind of collection of data communications, you would need to be very careful about how wide you open that up, de facto, without warrants—and pointed sticks.

Q414 Professor Peter Sommer: Ross is entirely right to raise the issue of disclosure. It would have to be disclosed if the data existed. I was involved in a case in front of the Solicitors’ Regulation Authority against a firm of solicitors employed by the content providers, who took a very aggressive approach to members of the public.

Q415 The Chairman: Thank you very much. I believe that the Scottish Office Agriculture Department would always want the right to check on dodgy sheep subsidy claims on Skye, which has been a long-standing practice, so I have been told. That will get me more hate mail from north of the border.

I thank you all very much. It has been a very long session but it has been absolutely fascinating. We are grateful to you for giving evidence today; we are grateful for your papers. If there are any additional comments you wish to submit to us, please feel free to do so. When you get home tonight, look at the newsflash which got me excited coming here, that Apple has lost 12 million subscriber IDs and all the addresses—apparently not through their fault but because the FBI had lifted them from Apple and someone has hacked into the FBI and lifted 12 million addresses.

Glyn Wintle: Are you aware of the follow-on from that? One of the identities is apparently Obama. Using those unique IDs, you can start to query other Apple services and find out what games are being played on his computer and certain other information. This is what starts to happen when you collect large amounts in one place: it is going to get lost.
Q416 The Chairman: It has been fascinating today. I thought that that was a fatalistic bit of news to hear before coming to this Committee. Thank you very much once again, lady and gentlemen.
WEDNESDAY 5 SEPTEMBER 2012

Members present:

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

Evidence heard in Private

Everything Everywhere [Jonathan Grayling], Telefonica UK [Bob Hughes], BT [Mark Hughes], Vodafone [Vodafone] and Virgin [Simon McCready] (QQ 417-508)

Examination of Witnesses

Jonathan Grayling, Head of Law Enforcement Liaison, Everything Everywhere, Bob Hughes, Government Programme Manager, Telefonica UK – O2, Mark Hughes, Managing Director Security, BT, Mark Hughes, Head of Corporate Security, Vodafone, and Simon McCready, Group Risk Director, Virgin.

Q417 The Chairman: Welcome to this session, ladies and gentlemen. Thank you very much for coming. We are starting early because you are all here and we have an awful lot of important evidence to get through today. I thank you not just for coming, but for your written submissions. If I may say so, they are more forthcoming than I had expected. I am very grateful for that. I hope in this private evidence session today the only people here are members of this committee, officials and parliamentary staff, who will all respect the confidentiality of this meeting. I hope in your oral evidence, you will be equally forthcoming and level with us, because that will help us at the end of the day get a better Bill through Parliament. We will be taking a full transcript—that is what our parliamentary colleague there is doing. That transcript will be checked with you. We have given a commitment that we will not publish willy-nilly, but if you would like to discuss any parts of it that you feel could be safely placed in the public domain—I think our officials have already discussed that with you. If you are content with that, I hope that we can crack on with our evidence session. First of all, could you just for our private record state who you are and your position, briefly, please?

Simon McCready: I am Simon McCready. I am group risk director at Virgin Media.
Mark Hughes (Vodafone): I am Mark Hughes. I am head of corporate security for Vodafone UK.

Jonathan Grayling: I am Jonathan Grayling, head of law enforcement liaison Everything Everywhere, which is Orange and T-Mobile.

Bob Hughes: I am Bob Hughes. I am the government programmes manager for Telefonica UK, which you probably know better as O2.

Mark Hughes (BT): I am Mark Hughes, the managing director of BT security.

Q418 The Chairman: Thank you. Our colleagues will be asking questions. Do not feel that you all have to answer every single one if you feel that another colleague has covered the point, but if you do not feel that the point has been covered, then weigh in and we will crack on. Can we start first of all with Mr Wright?

Q419 David Wright: Thank you. Welcome to this afternoon’s session. It is appreciated that you are coming along and giving evidence. I will open the bowling relatively gently and ask you what discussions you have had with government departments and other agencies on the draft Bill. Do you think in the formulation of the Bill that your comments have been taken on board? Perhaps we could start with Mr McCready.

Simon McCready: We have had a number of discussions, principally with the Home Office, albeit at a relatively high level to date. Those discussions are ongoing. They certainly have listened to the comments that we have made and any concerns that we have raised with them. They have assured us that they are committed to an ongoing consultation should the Bill progress.

Q420 David Wright: What were the major concerns that you raised?

Simon McCready: I guess one of our major concerns was around the third-party service provider data, and the provisions for the authorities to come to us to access that communications data if they were not able to get it from the third party themselves, who may be based overseas and not be subject to the same legislation that we are bound by. We could envisage a scenario in which it may be harmful to our commercial relationships with those companies if we were to be obliged to disclose data which they had already refused to disclose. We can imagine that having a commercial impact.

Q421 Mark Hughes (Vodafone): Very similarly, 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. Our concerns are exactly the same as Mr McCready’s in that, from a third-party services perspective, one of the things that we were really hoping to gain from that meeting was exactly which third-party services law enforcement and government have got relationships with, and which they have not. That has an impact on how difficult it would be and how much data we would have to be able to extract, store and then disclose on behalf of law enforcement.

Jonathan Grayling: Very similarly, we have had a number of high-level meetings with the Home Office previous to the Bill being published. We also had a very useful meeting with the Home Office, as industry, a week before the Bill was published, just to get a feel for what the
content of the Bill would be, and then a couple of meetings subsequently. Those subsequent meetings have been very helpful. We have had some of our questions answered, albeit verbally, but Everything Everywhere’s main concern really is, with regards to the scope of the Bill, how it actually looks on paper and how that aligns with what the Home Office are telling us verbally and what they are going on the record, verbally, as saying.

Q422 David Wright: So what are the gaps?
Jonathan Grayling: It is very similar for me to my two colleagues in relation to the fact that the Home Office is verbally saying that third-party service provider data is its key priority and that it will be approaching those third parties to require them to retain the data. We think that that is not explicit in the Bill. We think that the Bill is very wide-reaching and very wide in scope, and that it places a significant amount of obligations on us as telecommunications providers over and above the obligations placed on the service providers.
Bob Hughes: Our view is that we have had a huge amount of consultation when it comes to the capability gap or whatever you want to call it and the need for going forward—the requirements, if you like. To be honest, the Bill, which is the Home Office’s reaction to those conversations, is relatively recent. As my colleagues have said, we have had a couple of meetings since. One meeting was to tell us what the Bill would say and another later was to gauge our reaction. However, we hope that there will be an ongoing consultation and that this will not be the last of it. Put simply, there are a huge number of issues, as everyone here has said, especially around third-party data and data that is not relevant to our customers or even our virtual customers. To bring this up to date, it is not about only the acquisition and collection of that data—its security, maintenance and everything else, which would be an overhead for us—but the quality of that data and how much use it would add for the people interested in it and, in our view, how little of the capability gap it would actually close. There would be a lot of investment and work for very little benefit.
Mark Hughes (BT): We have been consulted in the same way as others have already mentioned. In the context of this type of legislation, it is worth mentioning that we are often consulted with all other types of legislation. We have an ongoing relationship with the Home Office, which has not been different in this case, at all levels within our company. Our concerns were obviously outlined in our written submission, which, again, others have mentioned. I would say up front that the broad scope of the wide-ranging nature of the proposed draft legislation is evident. Under that, I do not think that the Bill in its current form has enough checks and balances in terms of some of its mechanisms. At the moment, they are not clear enough to almost counter that broad scope. Therefore, if the Bill is enacted and we see these things working, some of the detail around how notices would be served and those mechanisms would work needs much more consideration in terms of the scope that you asked me about.

Q423 David Wright: So your concern would be that the Bill would proceed on to the statute book but that a lot of the work in terms of notices and the nuts and bolts of it would have to come later. I think that the Committee will be concerned that we do not have enough clarity through the Bill at the moment. Is that a fair summary?
Mark Hughes (BT): From my view, yes it is. I do not think that a lot needs to be done in the current draft legislation but some things could be done—certainly around the so-called
Technical Assurance Board and how that would work and the various powers of the Secretary of State. For example, in having read this, we cannot see any mechanism for us to object to a decision that perhaps would be arrived at under a notice other than judicial review. I do not think that it would be particularly helpful to have to go to that. It looks to me that something could be inserted in this legislation to make that process a lot easier to deal with at the time that the notice was being formulated and before it was enacted as the Bill currently outlines.

Q424 David Wright: What is your general view about the oversight of the powers within the Bill at the moment? Has anybody got a view of that in terms of process and assuring the public that that process is being followed effectively?
Jonathan Grayling: I think that the existing processes are already there under RIPA. There is oversight under RIPA and, certainly from our perspective, we think that the actual RIPA oversight process works and is sufficient. That is in relation to the appropriate authorisation processes within the law enforcement agency or the public authority. You have got the Interception of Communications Commissioner, who carries out his own checks and balances as well. One thing that perhaps needs addressing in the Bill is whether its powers will be abused by law enforcement and public authorities. That would give public confidence that there was something in the Bill in relation to the powers themselves being abused. There is already in place legislation such as that on data protection and the Computer Misuse Act which could be utilised. The sanctions that could be taken against telecommunications providers are mentioned in the Bill, but not specifically those in relation to individuals applying for the data.

Q425 David Wright: What do you think about the scope and range of organisations that can apply for data? Do you think it is too wide? Do you think that it ought to be limited to the security services and the police? Does anybody have a view on that?
Bob Hughes: One of the upsides of the proposal is that at the moment we have comms data requests that come in under all manner of different legislation. How people translate that data and what they think they can apply for is actually sorted out on the front line, which it should not be. So one of the real powers of the changes proposed here is that it all comes under RIPA. The oversight that we have in place is extended and increasing it would be really good. RIPA sets out the authorities that can apply. It is probably not our place to say as a CSP whether that is right—that is more of a political view—but it is very rarely abused. Our struggle is always to find whether this or that is correctly authorised and whether we should be releasing that data, and whether the person had the right authority level. If that is clear, that will make our day much easier than it is at the moment. The issue of whether magistrates will be able to increase the oversight as regards local authorities, or something like that, is yet to be seen, as far as I am concerned.
Mark Hughes (BT): I would just add that, like my colleagues, we absolutely recognise the fact, as Bob was just saying, that parts of the draft legislation tidy up the whole plethora of requesting authorities. We welcome that and it is a big step forward, as far as we are concerned, regarding the upside of the draft legislation.
The Chairman: Lord Faulks, you wanted to come in on this.
Q426 Lord Faulks: You have all expressed understandable concerns that the obligations that the Bill might place on your organisations are not entirely clear from the Bill. What I would
like to ask all of you—particularly you, Mark Hughes of Vodafone, with your background in fraud investigations—is: do you understand what the Government really want, and do you think it is a necessary and reasonable thing for them to seek, or do you really think that this legislation is something that is not going to help very much?

**Mark Hughes (Vodafone):** First and foremost, I think we have to recognise that there is a significant challenge for law enforcement investigations because of the fragmentation of the way that customers are communicating in this day and age. No longer are customers just making telephone calls and sending text messages. All our organisations connect customers to the internet, and then they can choose from a range of third-party applications to have those conversations. Because of the way that that is architecturally designed within our organisations, it is absolutely reasonable to suggest—although I do not know in terms of the amount of intelligence that is being lost from a law enforcement perspective—that that would be causing some significant disruption to the running of an investigation, because you would be able to follow the case up to a point but you would literally hit a brick wall and you would not be able to go any further. I would definitely recognise that that would be very frustrating in a number of police investigations into serious crime.

**The Chairman:** Lord Jones, did you want to come in on this?

Q427 **Lord Jones:** On the question of consultation, I ask the panel: when you have been engaged in your consulting with civil servants at a high level, were you ever promised a future meeting with a Minister? Are you able to define what you see as a “senior” civil servant, in terms of the grade of the person or persons you are operating with?

**Jonathan Grayling:** We have all had meetings with Mr Brokenshire, the Police Minister, so we have had meetings with a Minister. That was back in November last year, I think.

Q428 **Lord Jones:** Was that congenial? Did you get business done?

**Jonathan Grayling:** Yes. It was very high-level. Mr Brokenshire was using that meeting to look for our engagement rather than our support, I would suggest, and we have all committed to full engagement with the Home Office. We have an excellent constructive working relationship with the Home Office and always have done. We had that very high-level meeting with Mr Brokenshire and since then have all had meetings with civil servants within the Home Office. At what grade, I would not be able to comment, but they are our regular contacts, who we have been working with for years.

Q429 **Lord Jones** Do you feel you have had genuine consultation so far, at the appropriate level given the seriousness and importance of the issues?

**Jonathan Grayling:** I think we have had engagement at the appropriate level. The actual information and engagement we have been provided with prior to the publication of the Bill was also high-level. We did not get involved in specifics of the drafting of the Bill—in fact, when the Bill was first published, that was the first sight that we had of it. Previous engagement was very high-level, and subsequently the engagement has been very useful. The Home Office has answered our questions, so I am hoping that will continue going forwards.

**The Chairman:** Dr Huppert?
Q430 Dr Huppert: Thank you, Lord Chairman. It has been said before that oral agreements are worth the paper they are printed on. Both in what you have said earlier and in what you have submitted, quite a few of you have said that, in a lot of cases, what the Home Office has been telling you about its intention does not fit with what the printed text says. Are you starting to get some of that in writing or is there the risk that there is no permanent record of understandings which you had about how that worked? Bob Hughes?

Bob Hughes: We have got a very clear view of what we need to do and what our companies need to do to assist in filling the gap that exists. The verbal conversations have been around just what we are going to do in that area. The problem is that when it has been captured on paper, if you just go by the black and white, we could be asked for a huge amount of data that could stretch across a very wide band. When the Home Office came out to see us after it had been published, they said, “Do you see what we are trying to achieve?” We do see what they are trying to achieve but our concern is that, as it is written, when we have the conversation out here in a few years time, we will be left with a piece of paper that says, “Here guys, you all signed up for this really wide piece”. All the consultation was about the gap, what the requirements would be and how it was going to be filled. Then, as has been said before, we saw the draft Bill and commented right from the word go that this is very wide and could affect our businesses quite a lot.

The Chairman: Baroness Cohen, and then we need to move on.

Q431 Baroness Cohen of Pimlico: I have been brooding about the question of how you govern the relationship between the Home Office and the people it is asking to provide things. What would an arrangement you could live with look like? How is it going to turn out? Is it going to look like a memorandum of agreement or would that be well beyond your imaginings in dealing with the Home Office on security matters?

Mark Hughes (Vodafone): For me, what we need is to be trusted with some more of the detail that sits behind the principles in terms of how the Act is drafted at the moment. As everyone has said, we enjoy a good working relationship with the Home Office, who are usually brokering these policy changes that they wish to make. We have had regular meetings et cetera, right the way up to the Home Secretary. I think for us the frustration is that, until we can get the answers to some of the specifics around what this would look like technically and which third parties are in scope, it is really difficult for us to envisage what that will look like, what the impact will be on our businesses and how we can all make sure that we continue to support the police in the way that we all attempt to every day.

Q432 Baroness Cohen of Pimlico: Assuming you got all that—at some stage you will have to, possibly somewhere down the line when the Bill is nearly law—what kind of document would you be formulating it into? What would it look like—a memorandum of agreement?

Mark Hughes (BT): There is a very well established process for how the request is made at the moment, through the law enforcement single point of contact. It is a very well established process between us. I think the key thing to point out here, and the big difference, is that the Bill quite clearly now talks about the data that we would be required to generate, which is not data that we currently generate, on the basis that the current legislation that we exist under only deals with data that we collect for normal business purposes. We know what we currently generate and why we generate it but there may be a load of other data that needs to be
generated, although we do not know what that is yet. The mechanism that I am talking about, and which I referred to earlier, given that this is quite an open-ended thing, is the mechanism for how we agree and understand what that data is going to be and what technical measures we need to put in place, how much they are going to cost, how difficult they will be to implement, and the proportionality around that. That is where I think we are saying—I speak for myself here and BT—that the provision in the Bill is where we need the detail. Rather than relying on the current mechanisms, which work in the current existing legislative framework, they would need to be different because the purpose of the Bill is different. It is not talking about just dealing with data that we collect for normal business purposes.

**Baroness Cohen of Pimlico:** That is very clear, thank you.

**Q433 The Chairman:** So is RIPA the right vehicle to introduce these new concepts?

**Mark Hughes (BT):** RIPA gives a lot of the requirements and checks and balances, which some have already referred to and which have worked pretty well. I know I am going on to another point, slightly, but it is a point worth making: some of the definitions in the draft legislation are problematic and have been for some years in RIPA and current legislation.

**Q434 The Chairman:** I know we need to move on to other colleagues, but is that because the technology has changed but RIPA used terminology designed for telephone calls and text messages while we now have all the new internet stuff and are still using the same definitions of “traffic”, “content” and “subscriber”? Is that the point that you were making?

**Mark Hughes (BT):** Broadly speaking, in a nutshell, we are talking about the difference between communications data and content. In the newer, technical world, the need to distinguish between one and the other is quite important because they are governed by different pieces of legislation. This piece of draft legislation is specifically about communications data, not about content. That definition needs to be quite robust because, as you say, the technology has changed. We believe that that needs to be addressed more robustly in the way that the current legislation is drafted.

**Q435 The Chairman:** I think that my colleagues will wish to pursue that point later. Mr Bob Hughes, you said in answer to Mr Wright that there was a capability gap and that a lot of time, money and investment could be spent with very little benefit. I hope you recall that. What did you mean by it?

**Bob Hughes:** You will have heard that all of us have expressed concerns about third-party data. We have a real issue, apart from the fact that it opens a Pandora’s box and we do not quite know what is in there at the moment, because we just passed it on. The other issue is—I know it will come up during the afternoon anyway—that a lot of those data are encrypted. If we are starting to talk about encrypted data, let us go into an analogy. I am sorry that this is the same one as I always use. When we were looking at RIPA, we always knew what was communications data and what was content by comparison with an envelope and whether something was inside or outside the envelope. That has worked for us. It does not really matter what the technology is; we can keep going back to asking, “Am I now inside the envelope or outside it?” That works very well until you get to encrypted data and what we will see of it. 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 encrypted data. Therefore, the value, by comparison with the letter and its journey from A to B, is much reduced.

The Chairman: Thank you. I think I understand that, I shall read the transcript a few times.

Q436 Lord Armstrong of Ilminster: I understand encrypting the content but do you also encrypt the data?

Bob Hughes: If it is just point-to-point encryption—for example, if a letter was sent from A to B but was in a foreign language—you still get everything that you would have got in comms data. You would still get the address on the outside. However, if it is gateway-to-gateway, all those letters and communications are put into what we would call a VPN tunnel. It is something that passes across our network as purely a point-to-point communication. We do not see all the data within that pipe and would not be able to distinguish between the content and the data inside the envelopes.

The Chairman: Dr Huppert, a brief question; then we need to move on.

Q437 Dr Huppert: Just two things, quickly, I hope. First, just to make your example clear, which category would a Gmail or Facebook message be in? Would it be in one where you would get all the communications data, or would all the communications data be encrypted?

Bob Hughes: A Gmail message coming across the telephonic network definitely comes into that because it goes through a Gmail server. It is sent off to whoever the mail server—

Dr Huppert: So it is an encrypted version.

Bob Hughes: So we would not be able to tell you where it was going or how it was dealt with.

Q438 Dr Huppert: The question that I really wanted to ask, since we are in private session, was: can you give us some sense as to whether it is possible in any way to decrypt these sorts of messages in the way that the Home Office has implied? Is that technically feasible?

Bob Hughes: Only with the keys. That is what they are designed for. We would not have the keys. And of course it is proprietary encryption, so it is not necessarily just the keys. It could be that you have got to have the language with which to decrypt it.

Jonathan Grayling: I think the other issue is that, even if we were able to decrypt, you would have to open the whole packet, and then you are looking at the content. That is what the Home Office has been very explicit about, again verbally—that it would not expect us to touch anything that is encrypted.

Q439 Lord Strasburger: Who does hold the keys?

Mark Hughes (Vodafone): The provider of the communication, whoever is sending the communication, would hold the key.

Lord Strasburger: Gmail.
Bob Hughes: Yes. So if we go back to the Gmail example, Google will hold the encryption keys. It is only those guys who could give you all the separate letters in the box.

The Chairman: Mr Ellis.

Q440 Michael Ellis: Of course, those companies may have less of a severe system to protect that data than Governments sometimes set up, such as the British Government. That is possible, is it not? They might have, for example, internal access within their own head office that would allow the use of those keys without regard to the sort of protocols that a Government such as the British Government would establish. Is it fair to say that?

Mark Hughes (Vodafone): In some cases yes.

Jonathan Grayling: They would have their own internal processes.

Q441 Michael Ellis: Yes. So can I just move on to what data is currently missing? We have heard it said several times, including from senior members of the security apparatus, that 25% of data is missing. They estimate—and it can obviously be only a guesstimate—that, whereas 30 years ago, in the days of landline telephones, they were able to achieve a 95% or close-to-100% success rate when they wanted to counter nefarious purposes in telecommunications interception, now their abilities are reduced to the level of about 75%, and that will get only worse because of the advances in forms of communications data. So do you accept that that figure is approximately accurate? I appreciate that it can be only a guesstimate, but do you accept that that is an obvious statement of fact? Can I ask you that first? I will go on to the second limb?

Simon McCready: I do not think we would be in a position to say whether 25%, even as a guesstimate, is right.

Q442 Michael Ellis: Is it your instinctive feeling that that is possible, clearly knowing what you know about modern forms of communication—including Skype and all the rest of it—compared to 30 years ago when we just had landline telephones?

Simon McCready: I think it is possible. I would echo what Mr Hughes said earlier, and we can certainly see the rationale regarding data that is not currently retained by us which could be of interest to law enforcement agencies as they investigate crime. We can certainly see the rationale. We can see the logic in there being a gap. Whether the figure is 25%, 35% or a slightly smaller or bigger number is very hard to say.

Mark Hughes (Vodafone): Purely instinctively, I would say that it would perhaps be slightly less—

Q443 Michael Ellis: You would be happy to accept the ball-park figure?

Mark Hughes (Vodafone): I would say a ball-park figure. If it is not 25% now, from a future growth perspective, we are going that way. Whether it will be next year or the year after, I think we will arrive at that figure very soon.

Jonathan Grayling: I would echo Mr Hughes on that one, in that I think it will increase in the future. The indication that we have been given by the Home Office is that the gap, with regards to third-party service providers rather than ourselves, will increase and data will become more and more fragmented in the future, and I agree with Mr Hughes that that will increase to 25% or more, unless something is done.
Bob Hughes: If we look at it historically, probably the years 2008 to 2010 hit a new high as far as intelligence from communications data was concerned after the impact of the data retention directive and the fact that data was available. Certainly, if I look at the requests that came into our company, they were nowhere near the amount of requests that came in prior to 2008, and our data users are probably among the most sophisticated in the world as far as the law is concerned.

Q444 Michael Ellis: Who do you mean when you say data users?
Bob Hughes: People requesting that data—law enforcement or whoever it is. But even within law enforcement, there are people who analyse the data and use it, rather than the policemen themselves.

Q445 Michael Ellis: So what you are saying, Mr Hughes, is that they can get more now than they ever used to be able to?
Bob Hughes: They can get more now, and what is happening is that as their sophistication grows, the technology is again going away from them. So there is another step to take. We accept that.

Q446 Michael Ellis: So it is a never-ending cycle?
Bob Hughes: It is. You are chasing the ball.

Mark Hughes (BT): Interestingly, the current code of practice by which the single point of contact operates under law enforcement is such that they are discouraged from asking us for data which they know that we cannot provide. There are some more technically savvy—if you want to call them that—single points of contact, or SPOCs, who sometimes try and ask us for stuff, but that is not generally how it works. They generally only come to us and ask us for a disclosure request when they know that we are in a position to provide that data. So with regard to the gap, I really cannot speculate, because it is a very difficult question to answer. You are starting by saying that there is a whole load of data, then there is obviously a subset of that data that would be useful to law enforcement, and I do not know what that is, and within that there is the issue of how much of that is currently available or not. All I can say is that the way in which it currently works, under the current code of practice, is that they are discouraged from asking for stuff that they know that we cannot provide.

Q447 Michael Ellis: But it would be within your knowledge, though—would it not, Mr Hughes?—that there is material that they cannot currently obtain, and you know that they are not able to obtain that information because of your general knowledge in the area?
Mark Hughes (BT): There are two things: first, the fact that some of the SPOCs will ask us for stuff that I know that we cannot, under current legislation, provide; and secondly, the draft Bill itself is being written to deal with a much broader requirement for data.

Q448 Michael Ellis: So there is a need for the Bill. Clearly you all agree with that. As far as the current situation is concerned, to what extent do you think that your organisations, if I can put it this way, are responsible for the law enforcement community’s abilities being sort of less valuable in fighting crime? Can you do any more without this legislation—if you did not have this new Bill—to provide more information to law enforcement agencies in fighting
crime? Are you operating at the highest level of your ability in the current legislative framework?

**Mark Hughes (Vodafone):** I believe that we are, from a Vodafone perspective.

**Q449 Michael Ellis:** Are you co-operating in good faith, as far as you can, with law enforcement agencies?

**Mark Hughes (Vodafone):** Absolutely 100%.

**Michael Ellis:** I take it that you accept the public interest in achieving the best possible results in obstructing criminal affairs and terrorism.

**Jonathan Grayling:** From an Everything Everywhere perspective, we are fully committed to working with the Government and the Home Office in the prevention and detection of crime. We have an excellent working relationship and meet them regularly. We take the approach that we want to assist in the prevention and detection of crime. However, we balance that with the impact that it has on our business and our customers.

**Q450 Michael Ellis:** Conscious, as we all need to be, of the impact on your businesses, the Government are offering to make good the expenses of this operation, are they not? The taxpayer will pay for what is provided, will it not?

**Mark Hughes (Vodafone):** At present RIPA states that the Minister of State will make appropriate contributions. I have been involved in this area for around four years. 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. One of Vodafone’s concerns about the draft legislation is that we recognise how technically difficult this will be. Regardless of the detail that we do or do not have at this point, this is more difficult than what we are doing now. It will involve our storing a lot more data than we do now, which is expensive. Therefore, one of the things that we would like to see in future years—when, as someone mentioned, all the people in this room and in these roles have moved on—is that 100% being written down and more enshrined in the legislation. As we go on, it will become ever more difficult to make sure that we are complying as fragmentation continues.

**Mark Hughes (BT):** I would just like to pick up on the previous comment before we lose that. We have to recognise that within this space there is a data retention directive, RIPA and the current legislation that applies to communication data. There is also the Data Protection Act. We have to be careful that we do not fall foul of breaching it by retaining data that we are not allowed to retain [REDACTED]. We have to be very careful. We are absolutely as co-operative as we can be within the current legislative framework and comply with it to the best of our ability in BT, as many others have said before me. That is quite important: there are different pieces of legislation at work here.

**Bob Hughes:** Can I just pick up on the point about responsibility? You said that you felt responsible for the gap. All the companies represented here are switching and working to protocols that are on the global market but not necessarily designed by our companies. We have to provide services using the technology that we have. If we take something as simple as the mobile companies’ use of the internet, we are limited by things well beyond our control, such as the number of version 4.0 addresses that are available. That means that, instead of
every single call and transmission having a record, which we used to require for billing, we bundle. We say, “Okay, a particular customer will have a huge bundle of data. They are allowed to have that bundle and we will measure it”. If we do any limitation or billing, we will do so based on that bundle, not on anything else, because the bits are too small. It is not a case of our not playing the game. We have always provided all the data that we can. As has been said, we made available data that we had collected to bill our customers.

Q451 Michael Ellis: That brings me to my final point, which is: are you concerned that you might be required to hold data on communications for services for which you are not primarily responsible? If you are concerned about that, could you expand on it by giving me some examples of how or why that might happen?

Mark Hughes (Vodafone): Yes.

Mark Hughes (BT): The Bill is explicit about that being the case and being an eventual outcome. Certainly, from our point of view, the Bill is quite clear about the fact that so-called third-party data, to which some have already referred—

Q452 Michael Ellis: I accept that but are you concerned about it and, if so, why?

Mark Hughes (BT): Speaking for BT, I do not know whether to be concerned because I do not know what it would entail at this point. However, a concern that I have already expressed is that the mechanism by which we arrive at what we would be required to do is the one that could be tightened by the draft legislation currently proposed. That is: what is technically feasible and how much it would cost? That goes back to a point that Mark 1 made, which is that there is almost a proportionality element in the costs associated with it. That is, if those data are required from a third party, you need us to get them and we go through the notice process, the cost is then an element that must be clearly defined. To use your analogy, it would be disproportionate to have 200 police officers investigating a shoplifting incident if that were the outcome of trying to achieve a particular third-party data request.

Mark Hughes (Vodafone): May I add to that, please? I am concerned on two fronts from a Vodafone perspective. First, if we were to hold an amount of third-party data from big services—some of them have been mentioned today—such as Gmail, Facebook and so on, it would be a lot of data. That would involve our having to have bigger data stores. Property real estate, certainly for the Vodafone organisation, is at a premium. If I had to increase the size of the footprint of the data stores that we currently have to keep this information, it would be very problematic for me. In the data stores that we have, there physically would not be the space or power to connect them. We would have to look at re-siting them, which then becomes technically much more challenging.

Q453 Michael Ellis: The nature of that is that it can be anywhere, is it not? It does not have to be in a central London prime location.

Mark Hughes (Vodafone): No. We must have two sites. We must have a resilient site in case one site goes down. Physically, space is at a premium. How big the stores would need to be would depend on what the legislation asks us to keep from a third-party perspective. I have lost my train of thought on the second front.

Michael Ellis: Perhaps you could come back to it.
Q454 **Lord Strasburger**: Could you tell us exactly where this capability gap is and what difference the Bill would make if it were enacted?

**Jonathan Grayling**: I think that is an issue that has not yet come up, to be brutally honest. We have not had that detail, and that is the key part of the Bill itself. We understand that, from a Home Office and policing perspective, to disclose the capability gap would disclose the sensitivities around where that gap is, which could make criminals aware of what technology could be used to communicate. We understand that there is an issue there and that maybe the capability gap cannot be disclosed publicly.

**Lord Strasburger**: But we are speaking in private now and I think we need to know.

**Jonathan Grayling**: We have not been told what the capability gap is. We understand that it relates to the third-party service providers.

**Lord Strasburger**: So you do not see the capability gap; you are being told about it.

**Jonathan Grayling**: We are being told about it

Q455 **Lord Strasburger**: By whom?

**Jonathan Grayling**: By the Home Office. We are being told that the Home Office works closely with our respective industries and companies and that it will work with us to identify the gap on the data that we already hold. We work closely with them on that. What we have not seen is the make-up of that 25%.

**Bob Hughes**: We understand the gap from the point of view of where the technology is missing; it is the detail that is missing. For example, we know that the average user now does not carry one device—they carry two or three devices or might have a smart device that acts as two or three devices. The problem that the law has is that, whereas you used to be able to say, “Person A is on a given telephone number and is now in Pall Mall or Trafalgar Square”, that same device may pick up wi-fi, 4G or 3G. It may swap between suppliers and big network companies and down into something that is provided by the local coffee shop, so that it is swapping constantly. These are designed to be active devices so not only are they swapping, they are on e-mail and on the internet. There are many different elements to the communication that comes from one handheld device. They are more like a mini-PC than they are a telephone as we would understand it. The gap, if there is one, is that any element in that string of communication might be the key one that is being looked for.

**Mark Hughes (Vodafone)**: [REDACTED]

Q456 **Lord Strasburger**: Therefore, it is not the case that you receive 100 requests for data and you can satisfy only 75. Presumably you satisfy them all.

**Mark Hughes (BT)**: It is designed so that they do not ask us if they know that we cannot provide. That is specifically done. The code of conduct is that we are not asked.

Q457 **Lord Strasburger**: So you never see this gap?

**Jonathan Grayling**: The way it works is that, through the SPOC community, we, as an industry, train those SPOCs. We provide advice, guidance and training to the SPOC community about what data we hold as part of our respective organisations. That is very clear.
If there is any gap or anything that law enforcement requires of us over and above what we can already provide, we work in a consultation approach.
From a specific company perspective, it is a fairly robust, well documented process.

As I understand it, the gap that Bill tries to address is the issue with third parties and, specifically, overseas third-party service providers—for example, webmail providers and social networking providers—whereby that communication goes across our network but does not have the co-operation and the buy-in from those third-parties, either through a retention process or a disclosure process.

**Q458 Lord Strasburger:** You said that the volume of requests you had received shot up between 2006 and 2008. Is that because the usage of these devices has changed? When RIPA was first implemented, you got requests about only telephone calls. I presume that now you get requests about telephone calls, e-mail, web browsing, social networking and all other uses of the web. Does that mean that the amount of data within your locations that is available to the public authorities that might request it has gone through the roof?

**Bob Hughes:** It has.

**Q459 Lord Strasburger:** So is it true that the 75%, if it exists, is 75% of a much larger set of information? If so, do you know how much larger it is? Can you put a figure on it? Is it 10 times larger or 100 times larger?

**Bob Hughes:** Yes, it is larger.

**Mark Hughes (Vodafone):** I do not know the figure. It is important to add that during that time period a lot of communication service providers re-engineered their systems so that they were more automated than in the past. Instead of having lots of pieces of paper and a very bureaucratic process for the police to follow to get access to the information they needed, we all assisted with a lot of efficiency drives. Achieving some of that efficiency also contributed to an increase in the number of requests.

**Q460 Lord Strasburger:** But do you agree that if the 75% Home Office figure is accurate, it would be 75% of a very much larger set of data than was the case when RIPA was passed?

**Bob Hughes:** That is definitely true. Absolutely.

**The Chairman:** Thank you. That is helpful.

**Q461 Mr Brown:** We have not yet got to any detail that you do not, or you say that you do not, have.

**Bob Hughes:** We are used to that.

**Q462 Mr Brown:** But you must have some working assumptions. Could you say anything more to give us some better understanding of the sort of data that you do not hold for your own businesses purposes at the moment and that you believe the Bill under consideration will require you to hold on to for the purposes of the security services and other proper authorities that would want access to it? You must have some working assumptions.

**Jonathan Grayling:** [REDACTED]

**Q463 Mr Brown:** Can you give us an indication of the period of time?
Jonathan Grayling: It is looking for 12 months.

Mark Hughes (Vodafone): [REDACTED]

Q464 Lord Strasburger: So are you being invited to intercept data that is passing down a pipe that you never look into?

Mark Hughes (Vodafone): We would not have a business interest. It is not an interception. The Home Office or the police would have to say to us, “Here is a list of the third-party applications that we are concerned about”. That contributes to the 25%. Once we can identify the packets of data, we would need to find a way technically to say, “Okay, we understand that we now need to retain these”, but they are encrypted or not on an application-by-application basis. If they are fully encrypted, we need to be able technically to unpick it and say, “Here is the traffic data but obviously we have not touched the content”, which is very difficult.

Q465 David Wright: From the evidence you gave earlier, the encryption element would require you to go back to some of the organisations, such as Google.

Mark Hughes (Vodafone): If they have got the key and can provide it because they are friendly, that would be fantastic because it would make everyone’s life a lot easier. Depending on the service, some of the services may have the traffic data held in clear text. It is largely dependent on which third-party services law enforcement is interested in. Until we know the answer to that, it is largely speculation on our behalf.

Q466 David Wright: Therefore, you must have had some conversations with some of those organisations.

Mark Hughes (Vodafone): Do you mean with third-party service providers?

Q467 David Wright: You have not.

Mark Hughes (BT): We have to be very careful on the point about interception. In our world, interception relates to content. Nothing described just now was about content. It is about what website was visited, by whom and where they were. It is not about what went on in the exchange. We are specifically talking about communications data. Mark Hughes just described communications data relating to that. As regards the third party and keys, at the moment there is no provision under current legislation for that data to be disclosed and I have no idea whether there have been any interactions with service providers around keys or anything like that. As we envisage it, under this draft legislation, as far as I can see, we would in no way be responsible for dealing with that. Our involvement would be, “Please collect that communication data and then provide it under the provision of the Bill”. The rest of it, in terms of encryption, would be down to—I do not know—the Home Office. David Wright: I understand.

Bob Hughes: It also comes down to the fact that we know and love our customer data. We take on the security of it and everything else. We understand it. If you are talking about third-party data, if anyone came to us and asked for our keys, in no way would we give them.

Q468 The Chairman: Thank you. We are getting excellent information but we are making very slow progress.
Q469 Stephen Mosley: On third-party data, who is the data owner? Is it you or the third-party?
Bob Hughes: It is the third party. We simply transmit the data.

Q470 Stephen Mosley: But you are not because you are being asked to store it. Who is then the legal owner of that data?
Bob Hughes: Going back to the box with the letters in, we will only store anything that is visible on the outside of the box. That is why we believe that it is low-quality data. It tells you only about that one transmission that went across.
Mark Hughes (BT): I think that the Data Protection Act is clear on the various relationships about data controller and data originator. We are not the data owner.
The Chairman: Thank you very much.

Q471 Craig Whittaker: Is it fairly safe to say that, if you guys do not know what the 25% gap is, the Government’s figure of £1.8 billion over 10 years is a finger-in-the-air job?
Bob Hughes: We do not know how the figure was created so we cannot comment.

Q472 Craig Whittaker: If you do not know what the 25% gap is, is it correct that you do not know what the costs of storing, retrieving and doing what you would be required to do will be?
Mark Hughes (Vodafone): We have never been consulted on cost.

Q473 Craig Whittaker: Okay. My real question is about your service users. What do you think that the impact will be on them when they know that you are having to store and perhaps disclose some of the data that you are being asked to deal with?
Mark Hughes (Vodafone): I think they will be very concerned.
Jonathan Grayling: I think that that is a key area of transparency with regard to our obligations. There is a potential conflict here between what is required under the Bill and our obligations to our customers. The Bill states in black and white that notices served on us will be secret. The data that we would be required to retain would be secret and we would not be required to disclose it. That is at odds with our commitment to our customers about what data we are retaining on them. There are operational issues as well, if we are retaining certain types of data, with regard to how we comply with data protection requests and subject access requests from our customers? How do we comply in relation to other statute legislation in courts whereby we would have to know what data we are retaining? If a court ordered us to disclose data, that would probably be in public: we would then have to disclose the data that we are retaining, which would be out in the open anyway, within the court. There appears to be some conflict about the secret nature of the notices and the transparency and the operational issues afterwards.

Q474 The Chairman: Is that worry shared by all of you?
Mark Hughes (BT): I will just say that the draft Bill makes reference to disclosure under the Freedom of Information Act and the fact that this data, if retained under the legislation, would then be exempt from the Freedom of Information Act. But as Jonathan has just said, there does not seem to be a commensurate realisation that the data-subject access request
under the Data Protection Act would be a route for someone to get to the information in any case. I see that as a current issue in the draft legislation, which would have to be tightened up and closed down. Otherwise, you are almost circumnavigating the intention of the Bill.

Q475 **Craig Whittaker:** Do you think then the public would be better served if they were required to publish the notice rather than keeping it secret?

**Mark Hughes (BT):** [REDACTED] As I understand it from what law enforcement and others are trying to achieve here, I do not think it would be useful for the people who law enforcement might be interested in to know what notices are being served on us, because that would give some degree of insight into what law enforcement is trying to achieve. From our point of view, that would be difficult for us, in terms of a level playing field about who is being asked for what between different service providers. [REDACTED]

Q476 **Craig Whittaker:** Does everyone agree?

**Bob Hughes:** The more sophisticated criminal, whoever they may be, will be looking at the notices and going to somebody else. And if anybody thinks there is a privacy thing about it, they will do the same, so we will see customers move.

**Mark Hughes (Vodafone):** I agree. The only thing I would add—and I do not want to sound like a stuck record here—is that in terms of these notices and whatever they look like, instead of waiting until this Bill runs its course, we need to get sight of those services as soon as possible.

Q477 **The Chairman:** The secrecy point is interesting. Do you seriously think, in this day and age, that within minutes of those notices being served on, say, the five of you and 22 others, the internet is not going to pick up somewhere who has not got them? Are you convinced that who has been served a secrecy notice can be kept hush-hush?

**Jonathan Grayling:** I think there is a very real risk that keeping the notice and the content of that notice secret is going to be very difficult, not through leaking or anything like that, but simply because of the operational aspects and the impact it will have on our business subsequently and how we comply under other pieces of legislation.

Q478 **Lord Armstrong of Ilminster:** What would you say if a third party said to you, “Are you disclosing my communications data to law enforcement in the UK?”. What would you say?

**Jonathan Grayling:** Now?

Q479 **Lord Armstrong of Ilminster:** No, if this happened—if this legislation was passed and you had a secret notice put on you?

**Jonathan Grayling:** There is nothing in the Bill that addresses the tipping-off aspect. There is nothing in RIPA at the moment either—that is, about notifying a customer if they make a request of us about whether we are disclosing their data.

Q480 **Michael Ellis:** So could you do it now?

**Mark Hughes (Vodafone):** [REDACTED]
Q481 Craig Whittaker: Can I just ask you about innovation and the future development of new features for the internet? Some witnesses have told the Committee that the draft Bill might impair innovation, because of the collection and retention et cetera. What is your opinion on that?

Mark Hughes (Vodafone): Our view from a Vodafone perspective would be that, right now, pre-this legislation, we have to clear a number of hurdles before we can bring new products and services to market, to make sure they are compatible with our obligations under RIPA. That would be exactly the same if this legislation were to go through. However, the bar would be higher, essentially, so if there is more technical capability required in complying with the legislation, it would potentially slow down the launch of new products and services while we made sure that we could comply with it. Our agility to innovate would be hampered. I think it is reasonable to suggest that.

Q482 Craig Whittaker: Have you done any evaluation on how much it would be hampered?

Mark Hughes (Vodafone): Until we know the detail, it is difficult to say.

Mark Hughes (BT): Importantly, going back to the mechanism of how the notice is formulated, the discussion and the way in which the process works is currently very loose in the draft legislation. At the moment, the only mechanism, which is basically taken from the existing legislation, is the technical advisory board, which as I see it would have to be much broader than a technical advisory board. Dealing with proportionality, and the way in which we would then have the ability to contest that, is important. What is important within that, and I have mentioned it before, is the cost-recovery element of that. There has to be a mechanism for cost recovery. It is not a question of the fact that we cannot and do not make money from this under current legislation—we do it purely on a cost-recovery basis and that is very important to understand. [REDACTED] In some respects, the cost element is quite important, which is why we at BT think quite clearly that a very loose way of describing “best endeavours”, for want of a better description, of appropriate cost recovery, is not good for anyone. It would be much more sensible to have a much crisper definition around how that cost would be dealt with. In some respects, that would drive you down and answer a series of other questions around what is proportionate and therefore, technically, what we would be asked to do. If there then would be a situation where somehow we would become uncompetitive, or less competitive, because it would be more difficult to bring products and services to market, there would be a cost associated with that, which would be potentially prohibitive.

Bob Hughes: I would just like to say that the open nature of the UK communications market means that it is probably one of the most innovative in the world. You only have to go back relatively few years, when all of our competitors would be represented by most of the people sitting on this bench today. Now, we do not know where our competitors are. They could be as big as a global corporate working out of San Francisco or somewhere, but you can also launch an application on the internet from a back room somewhere. We are still competing but the problem is that the backroom guy does not have any of these constraints. He can get to market in two days and have himself a few million pounds in the bank by the end of the week, while we are still looking at what we have to comply with. The more that we have to comply, it slows us down, day by day.
Craig Whittaker: May I finally ask you about the Everything Everywhere statement that the solution for generating and gathering data could affect the quality and the speed of communications. Do you think this is a risk?

Jonathan Grayling: I think until we have further detail on what the requirements are and what potential solutions will meet those requirements, it is difficult to say. The point is that it could be a risk. If you take a very basic scenario in which we are required to capture huge amounts of data that are traversing our network, there must be some capturing capability to do that. If you put some form of capturing capability on the network, there is a risk that all data will have to flow through that and there is a risk that it could, potentially, slow down that data transmission. Until we understand the further detail and solutions, I cannot go into more detail; and until we actually implement solutions, you cannot test it. But I think it is worth raising with the Committee that it is a risk and it could potentially slow down the transmission of data.

Mark Hughes (Vodafone): Let me add to that as well please. If you imagine right now—

The Chairman: There is a Division in the Commons, which our Commons colleagues will need to attend. We will need to suspend so can we switch off the transcription please. We will reconvene as soon as two of you are back. That is not the norm, but I am conscious of how much we have to hear today. It will probably take about 10 minutes, but the faster we get back, the sooner we kick off.

The Chairman: Mr Brown, you had a question.

Q484 Mr Brown: Do you see within this confidential relationship between the security services and yourselves any need or requirement for some form of appeals mechanism so that you would have the opportunity to say, “We think this request is unreasonable or disproportionate or too technically difficult”, or to raise issues of that kind? Or are you satisfied with the way it is all currently structured, which seems to mean that you have an obligation to comply with whatever request is made?

Baroness Cohen of Pimlico: If you pay for it.

Jonathan Grayling: Is that specifically in relation to the requests made of us to retain the data, or the requests made of us to disclose the data?

Mr Brown: No, I meant on an individual requests.

Bob Hughes: Disclosure.

Mr Brown: To disclose.

Jonathan Grayling: I think we all agree that the existing RIPA process is pretty fit for purpose with regard to the appropriate designated authority or designated person within each individual public authority.

Q485 Mr Brown: You think it is contestable?

Bob Hughes: I am not sure that we would know enough about the case to contest it. That is the whole point of the request that is coming to us.

Mr Brown: That is also the problem for the person whose information it is because they do not know either, and that is probably what lies behind the thousands of requests that we have all received as parliamentarians—to protect the privacy of our constituents.

Mark Hughes (Vodafone): What we can do and what we do do—especially when we meet the Interception Commissioner—every year now is a comprehensive review of how much information we have disclosed, what we have disclosed, which forces we have disclosed it to
and how many hours of data they asked for. Then we share that with the Interception Commissioner so that we can flag that we now have it right in relation to the disclosures that we have made. It is then down to his organisation, while it is going around doing its audits, as to whether it wishes to do a more thorough audit of one force than another. It can do so if it wishes.

**Lord Faulks:** You can have judicial review if there were some generic request that was unreasonable.

**Jonathan Grayling:** Yes, but as Bob Hughes said, we would have no insight into or visibility of the purpose of the request.

**Q486 Mr Brown:** Yes, I do not quite understand the judicial review point, because how would the person who perhaps wanted to conduct the judicial review know?

**Lord Faulks:** Yes. You would try and compel them to give reasons.

**Mr Brown:** Sorry.

**Lord Faulks:** If they did not give reasons, there would then be questions as to whether there were adequate reasons and so on.

**Q487 The Chairman:** Before we leave this section, I have one question for you. You all have said that you have lots of communications dialogue with the Home Office, but nearly all of you orally, and most of you in your written evidence, have commented on your concern about how it could limit innovation and cause possible damage to your companies, and maybe slow down communication. Have you raised any of these concerns with Business, Innovation and Skills, our internet tsar, e-mail commissioners or whoever it is? Have you raised those concerns with any of the involved Ministers from BIS? Have you had any discussions about those concerns with the business and industry department. No? Okay? That is fine. That is all I wanted to know.

**Q488 Lord Strasburger:** I want to talk about storing data and the risks involved in that. You store a lot of data that currently you either dispose of or just pass through. Would that new activity introduce new risks of any kind that you can see?

**Simon McCready:** I think that storing additional data results inherently in some level of greater risk. I do not think that it is fundamentally different from the situation now, whereby we store and protect critical data of different kinds, complying with existing legislation. I think the answer is yes, there is some additional level of risk but not a fundamentally different one from that which we currently manage.

**Q489 Lord Strasburger:** What risk are you talking about?

**Simon McCready:** Just that storing more data results in the potential for human error or system error, resulting in that data becoming either corrupt or inappropriately disclosed.

**Q490 Lord Strasburger:** What about malicious attack?

**Simon McCready:** Possibly.

**Mark Hughes (Vodafone):** I was just going to add that owing to the potentially controversial nature of the information additionally needed to be stored by our organisations, and the fact
that there may be some hackers or activists who take umbrage at that, we may all become
greater targets for people who want to access or expose that data. I think that that is a real risk.

**Jonathan Grayling:** Generally, going on from what my colleague said, the more data you store
the more risk there is of breach. The less data you store, the less risk there is of breach. So it is
a simple matter, exponentially, whereby the more data we store the more the risk will increase.

**Bob Hughes:** You have also got the point that the data that we currently store is centralised
and is repeated throughout our business, so it will be in a billing system somewhere or it will
be used for some other purpose. It is therefore data that is more generally available. Now we
are saying that we will specifically collect data that we do not require for a business purpose. If
we have not required it for a business purpose, someone has probably has made a business-
need evaluation on that data and concluded that storing it has no value within the business.

**Mark Hughes (BT):** I do not have a lot more to add, except that that is one of the things that
needs to be factored into the process of consultation around formulating the notice—the risk
associated with the storage of different types and the amount of data. There is clearly lots of
data that we have to store and protect at the moment. That is not an undue concern; it just
needs to be factored into the process of formulating the notice.

**Lord Strasburger:** Is there another factor here that would make it more risky? As well
as there being a lot more data, the data would be a lot more sensitive. At the moment, you
effectively are storing people’s telephone bills. Some criminals might find that interesting, but
not many; but now you will be storing much more sensitive information about people’s
lives—where they go on the internet, their e-mails and so on.

**Mark Hughes (BT):** There is a lot of data that we have to store that is very sensitive and there
are a lot of techniques to ensure that we put in proportionate levels of control around that
data. That does not unduly worry us. Again I come back to the point that during the process
of understanding the implication of the notice, there would have to be due consideration
given to saying we now need to have petabytes in information stores that are particularly
sensitive. That would clearly come with quite a degree of cost of control to ensure that it was
proportionately protected.

**Lord Strasburger:** Would retention of more data for a lot longer cause you any
technical difficulties?

**Mark Hughes (Vodafone):** I do not think it is technical difficulties, necessarily. I think that it
is just cost. More data equals much more expense, to build it and to run it every year.

**Jonathan Grayling:** On top of that, there is the querying aspect. The more data that you store,
the more data there is to query. Again, that would be additional cost because you have to
develop the querying techniques on top of that.

**Bob Hughes:** There is nothing in the Bill as it stands that is not technically feasible. It is just
throwing enough money at it.

**David Wright:** Where would you geographically store this additional data? Would you
be storing it in the UK? Would you be storing it abroad? What happens if an organisation
decides to store the data in India? Does that come under the jurisdiction of the Indian
Government? Can they access it? That is a genuine question.
Mark Hughes (Vodafone): Operationally, it is all stored in the UK. I do not think that we would be allowed to store it overseas even if we wanted to.

Bob Hughes: We work currently under the data retention service specification, which defines that it has had to be stored within the shores of the UK and is currently one of the costs. Just about everybody here works globally, and it would be an awful lot cheaper to store it somewhere else an awful lot of the time.

Q494  Lord Strasburger: Can we talk about disposing of data? How confident are you that you will be able to meet the requirements to dispose of communications data at the appropriate time, and in such a manner that it cannot be retrieved?

Bob Hughes: Very confident. From a technical point of view, we shred data in the same way as if you put it through a paper shredder. There are degrees that you can shred it to so that it cannot be recovered.

Q495  Lord Strasburger: So you overwrite it?

Bob Hughes: A lot of the time when you think you have disposed of data, all you have done is take away the headers. We do not do that. We completely obliterate it. It is, again, technically very feasible. It is what we do already with billions of call data records per day.

Q496  Lord Strasburger: We heard from some industry experts yesterday that there are difficulties in destroying data, largely because there are back-ups of it on resilience systems. The operating systems might create their own back-ups that you are not in control of and so on. Are you sure that you can destroy every copy?

Bob Hughes: If you talk about massed data generally what they are saying is absolutely correct, but we are not. We are talking about data that is stored for a specific purpose, and therefore disposed of under specific rules. We build systems that are purely for data retention for these purposes, so we destroy under the rules that we set within our company policies for disposal.

Q497  Lord Strasburger: Are you all that confident?

Jonathan Grayling: Yes. I think the Bill specifies that the data must not be able to be retrieved again. I think that that is a very stringent form of wording. Your technical witnesses yesterday will talk in more detail than I can, but data could potentially be retrieved if you chucked enough money at it. The only way that you can actually guarantee that data is destroyed is by physically destroying the media that it is stored upon. If you overwrite the data, it could potentially be retrievable with enough technology and enough money. Practically, it is nigh on impossible but, if you again take the Bill in black and white—to destroy data so that it cannot be retrieved again—the only guaranteed way is by destroying the media that it is stored upon.

Q498  Lord Strasburger: So would you be doing that?

Jonathan Grayling: That would be an extortionate cost.

Mark Hughes (Vodafone): We would not be doing that, but we are all very experienced in making sure, under the current obligations, that it is not retrievable by either ourselves or law enforcement without some disproportionate amount of effort and money. We are all really experienced in that. The other unknown factor is, technically, the art of the possible in 10 years’ time from a forensic technology perspective. The broad answer from our perspective
would be that we are all really experienced in making sure that it is not accessible to either ourselves or the police.

Simon McCready: We would agree entirely.

Bob Hughes: We have to define the data that you are calling “sensitive” as well. The mass of the data stored in the systems is just ordinary, everyday weblogs. There are billions and billions and billions of them. You are talking about a very tiny piece of data that would be of interest to somebody. Then you also have to look at the data that has been requested. That is where we are very nervous, and make sure that we have done everything that we can to—not quite physically—destroy it. The very fact that it has been requested means that it could have been involved in an inquiry of some sort or other, so we have to step up the assurance.

The Chairman: We need to move on.

Q499 Lord Armstrong of Ilminster: We have talked a bit about the distinction between communications data and content. It is very significant in the Bill that content is out. The Bill is just interested in communications data. Are you confident that you can always distinguish between communications data and content in these activities? Are the DPIs and so on that exist able to do it? Do you have the people that can do it?

Bob Hughes: It all comes down to the definition and the guidance we get about where that line exists. Currently, there is debate. If we just take a simple web address, there is debate and disagreement as to where the line between content and the comms data sits, and has been for the last few years. We could not sit here and say that we are confident that it is clearly defined within the Bill or any other piece of paper at the moment. It is something that we could struggle with. We all have tools that, if the definition is good enough, we can absolutely bring it back without any problem, and it would be a repeatable situation. But it is absolutely dependent on the definition. So, if we take an ordinary web address, the guidance that is given at the moment is that, up until the first slash—www.ebay/—we call that the comms data. Everything beyond that, which could talk about details of what they searched on within eBay, is noted as being the content of the web address. There are people who come to us and say, “Actually, if you look at that, if it’s www.keekoo, which is itself a search engine which goes to Debenhams or somewhere else, you’re still only talking about a domain”. We ought to be able to say that keekoo/Debenhams is still the comms data, the address. But there is no real agreement because, according to the guidance that we have at the moment, it goes up to the first slash, so we would not be giving them Debenhams.

Lord Armstrong of Ilminster: There is a fuzzy line.

Bob Hughes: Yes.

Q500 Lord Armstrong of Ilminster: It is very important philosophically, you might say, that content is out in the Bill. But it is not as easy as that, really, is it?

Bob Hughes: No.

Jonathan Grayling: Especially for third-party data, which we will not have any understanding or interpretation of. 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.
Mark Hughes (Vodafone): The best people to store and disclose the third-party data are the third parties. There is no doubt about that.

Q501 The Chairman: Is that fuzziness because this Bill is trying to use the terminology of RIPA? Are you suggesting or implying that we should perhaps have different definitions or different terminology for the whole thing?

Jonathan Grayling: I do not think that it is RIPA necessarily, or even this Bill. I think a concerted effort of understanding what is communications data and content needs to be undertaken generically anyway, irrespective of RIPA or this Bill.

Q502 Lord Faulks: You all operate, to some extent, globally. The laws of other states and countries impose obligations on you, quite apart from anything that may actually or prospectively be imposed on you by this Bill. I know that you, Mark Hughes BT, said that there are some difficulties in trying to comply with the various existing legislative requirements. Do you think that what you are going to be prospectively required to do by this legislation is greater than anything that you are required to do elsewhere in other countries? How does it compare?

Mark Hughes (Vodafone): From a Vodafone perspective, we operate in 23 different markets globally. I would not say that there is a standard model, necessarily, for how we would cooperate with law enforcement in those territories. Talking to international colleagues, I would say that the relationship between law enforcement, government and telecommunication companies in the UK is the best in the world as far as we can see. That is due in no small part to the arrangements for cost recovery that are in place for 100% at the moment. In countries where there is not a cost-recovery regime, there is no way that you would get the turnaround and speed of requests. Not only are we storing this data, but with the SLAs that we operate under, such as a grade 1 life-at-risk request that we would be asked for, the police would expect that back within 60 minutes. When you are dealing with the many billions of records that we have got right now, and we need to turn those around at that speed, from a Vodafone perspective, other markets that we operate in would not get the same level of service.

Bob Hughes: I have worked in 33 countries in this area, and nobody provides the service that the UK does—not above the line, anyway.

Baroness Cohen of Pimlico: We pay for it.

Q503 Lord Faulks: Yes, because we pay for it, as the noble Baroness quite rightly says. There are potential conflicts of law in terms of the obligations that you might have, in terms of being asked to disclose data by this legislation and elsewhere being told that you cannot disclose the data. Those conflicts exist anyway. Do you think that there will be a particularly difficult potential conflict provided by this Bill? Can you envisage that there might be? It is something that you adverted to in answer to the very first questions this afternoon.

Mark Hughes (BT): I think, from our analysis, it comes down to the notices and how they are formulated. As I understand it from the draft legislation, the notices will be subject to further parliamentary scrutiny. That is why I think that that would have to be ironed out. We cannot see a headline—other than the things that we have already drawn out here around definition, purpose limitation and other aspects of the draft legislation—that it would be in direct conflict
with others. I have made the point around the Data Protection Act and data subject to access requests, which is the only area directly where I could see that there might be some difficulty.

Q504 Lord Faulks: I have just got one other general question, Mr Chairman, if I may. You have all discussed the problems, the obligations and the fact that you do not always know quite what those obligations are going to be. Can any of you think of any commercial advantage to any of you as a result of this legislation if it came into force?

Mark Hughes (BT): Briefly, I would say that there needs to be clearly in the Bill a requirement that the purpose limitation around the data that is collected under the notice ensures that it is only to be used for the purpose for which it is intended, which is to support law enforcement, and should therefore not be used for other purposes. That does not appear in there at the moment as far as I can see, and it should do.

Mark Hughes (Vodafone): My only add-on to that would be that the current data that we retain, and the systems that we retain it under, have obviously been built for the specific purpose of serving law enforcement. There may be, were each of our companies a victim of fraud ourselves, because of the way in which this data was collected and the speed at which it was collected—and the detail in which it is kept may be different to what we keep for our billing purposes—a commercial opportunity to, still for law enforcement purposes, use that and make sure that we take it to the police so that we can recover any fraudulent activity against our own businesses. That would be the only case, I would say.

Jonathan Grayling: I have one very quick point in relation to the international issue. As we understand it, the Home Office has commissioned its own international study into how this has been approached in other countries. We have had no visibility of that. I think that it would be very useful if that could be made visible.

The Chairman: This committee would find the same thing as well, actually.

Jonathan Grayling: And potentially to UK citizens, because I am sure that they would be interested in how it is conducted on other countries as well.

Q505 The Chairman: You mentioned the international aspect. I assume that if you and other companies had orders served upon you, irrespective of whether the wider world finds out, Mr Google and Mr Facebook may discover it. What if, hypothetically, they then publish on Facebook that they understand that if you go with Vodafone, BT or other companies in the UK, the Government will be able to access all your information and, therefore, they recommend that you use Blencathra e-mails.com? If they do that, what happens? Can it be done?

Jonathan Grayling: If they choose to utilise encryption technology, because of that very fact that they know that UK telecommunications providers have been obliged to retain this type of data, then we go back to the encryption issue, whereby the data is not visible.

Q506 Stephen Mosley: I was going to ask about the filter. The legislation allows the filter to go off to a third-party organisation. We assume this third-party organisation will be government, but it might not be. It is not specified. What sort of issues and what sort of difficulties would they encounter in being able to set up this filter, use it and access your systems?
Mark Hughes (Vodafone): In the first place, a filter, from our perspective, could be seen to be a good thing. Right now, if a police force was investigating, let us say for the sake of argument, three murders that had happened in three locations, they may come to our organisations and say that they need to know all the people who were in this location, using this cell tower, for this date and time. That may be many hundreds or thousands of people. If you had to do that three times across all our networks, you can imagine that a lot of collateral intrusion would be passed to the police. Our understanding of how the filter would work from conversations with the Home Office so far, and the questions we have asked, is that the filter would essentially be able to answer the question of the single point of contact; and that these are the people who were commonly in the three locations at the time, so that it gives the police only the information that they require, as opposed to all the other collateral intrusion that you would get from that request. Whoever this third party is, be it a third-party private contractor, government or law enforcement, or a mixture of the two, I think the problem would be the continuity of evidence. Right now, we are all used to going to court and defending our data in front of a jury of 12 people, who do not have an understanding of the way that telecommunications networks operate, so that we can help whoever the prosecution is in securing that prosecution. From a third-party perspective, whoever is operating that third party will absolutely need to be part of the witness process. We would not necessarily be able to say anything other than that we retained this packet of data and passed it to a filter. We would not necessarily understand it as well as we would our own data, so it becomes more complicated from an evidence perspective with the filter. That would be our view.

Bob Hughes: To add to that, we are passionate about protecting our customers’ data, as you can imagine most of us here would be. While we welcome the idea that we are not now handing over lots of innocent data that is just collateral to the request, it also means that we are handing it over to another body and we have to rely on them to look after it. That is no different from what we do at the moment when we hand it to the police, other than the fact that you change the perception of the proportionality. While the cell-dump-type request is relatively rare at the moment, if the proportionality question is answered and it is viewed that we are going only to end up, that might happen an awful lot more. There are two problems with that. First, that is an awful lot more data that we are handing over to somebody else to protect on our behalf. The second problem is that we then have to store more sensitive data for our gold copy, as they call it. So there are other storage issues and everything else that will pop out of it. But generally, it is seen a good thing.

Stephen Mosley: Under the current system though, they need to come to you and fill in the relevant forms. You get the request and then you have a choice almost—does this comply with it or not? You then have to make that decision. If it is an automated filter or system, you are not in there physically saying that you do not think it complies.

Jonathan Grayling: I do not think it is going to be automated, is it?

Bob Hughes: The filtering will be automated, but the request is not. They will come to us with exactly the same request. Using Mark’s example, it will be, “Can you give us the data on three cells, at three different times?” We hand all that data over and the automation means that it goes into a request filter and brings out only the one device that was in the three different cells. So there is no difference in the request; that remains the same. The difference is in the answer to the request—the single point of contact that requested it only gets back the specific.

The Chairman: Was there anything else, Mr Mosley?
Stephen Mosley: I was going to ask something on encryption, but I think we covered it all earlier.

The Chairman: Lord Strasburger had a point on encryption.

Q507 Lord Strasburger: Yes, you told us earlier that encryption makes it difficult or even impossible to distinguish between content and data. What is your understanding of how encrypted data is to be handled. Is it to be retained or not?

Jonathan Grayling: Explicitly not.

Q508 Lord Strasburger: Who has told you this?

Jonathan Grayling: The Home Office. That was in verbal assurances—it is not documented in the Bill. That is a key point, which needs to be documented within the Bill itself—encryption technology or encrypted data is out of scope.

Mark Hughes (Vodafone): There was a very slightly different understanding for me, although it may just be the way that we asked the questions when we met up with the Home Office. Mine was that we would not have to decrypt any data that was encrypted, but that we still may have to store it in its encrypted format and the encryption would be somebody else’s problem. I do not know if that was something that Mark was talking about earlier but I had a slightly different understanding.

Mark Hughes (BT): I have not had the feedback, but I thought it was that we may well have to retain encrypted data but that we would certainly not be responsible thereafter. The problem, which has been pointed out already, is how you separate content and communications data. With encryption, you would not know what you were handing over. That, obviously, is the problem.

Jonathan Grayling: May I just make the point that if—again, there are obviously different interpretations of our verbal discussions with the Home Office—we are required to store encrypted data, we could be storing content, which is illegal? That is why Everything Everywhere has been very explicit in getting confirmation from the Home Office that encrypted data is out of scope. If we were required to store any data whatever and there was content in it, that would be illegal. We do not know what is in it.

Lord Strasburger: The very fact that you seem to have differing interpretations of similar verbal discussions backs up your statement that it really needs to be written down.

Bob Hughes: It is all down to the definition.

The Chairman: That seems a good point at which to stop. We are all very grateful to you today for giving us extensive evidence and for backing up your excellent written evidence. You have also given the Committee and our officials a headache in that what you have told us today will help us come to our conclusions, but we will respect your confidentiality and we need somehow to agree with you and find some way to get the guts of what you have told us into the public domain. We will want to discuss that with you to see how we can, while respecting your confidentiality and the fact that you have talked to us frankly, somehow produce the evidence you have given us today in a safe form that does not damage you commercially, but at the same time justifies some of the conclusions that we will reach. Thank you, and your colleagues behind you, very much once again. It has been an excellent session.
IPSA [Nicholas Lansman], LINX [Malcolm Hutty] and Jimmy Wales (QQ 509-546)

Examination of Witnesses

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.

Q509 The Chairman: Welcome to our panellists and to members of the public. We are in public evidence session once again. Before I ask you to introduce yourselves, perhaps I may explain for the benefit of any watching media that our panel is a slightly odd mixture today in order to fit in all those who are giving evidence. We have two representatives of associations and Mr Wales, who is here in a personal capacity. Can I ask Mr Hutty to say briefly who you are?

Malcolm Hutty: My name is Malcolm Hutty. I am the head of public affairs at LINX, the London Internet Exchange, which is a membership association for people operating internet networks in the UK, including connecting in the UK from abroad.

Nicholas Lansman: I am Nicholas Lansman, the secretary-general of ISPA, which is the UK’s internet trade association. We represent about 220 ISPs—about 98% of the market by volume.

Jimmy Wales: I am Jimmy Wales. I am the founder of Wikipedia and, as was mentioned, I am here in my personal capacity.

Q510 The Chairman: Thank you all very much. I am sorry that we are running slightly late. The previous evidence session overran, interrupted by a vote in the Commons, and I suspect we may overrun slightly in this one, too. Perhaps I may kick off by saying that the Government have identified two specific issues about the present law that they want to address: it does not require communications service providers to generate and/or retain communications data for which they have no business need; and it does not apply to
providers based overseas. Do you consider that these issues need to be addressed in the Bill, and do you think that the way that the Government are going about addressing them in the Bill will impact heavily on the operations of the industry?

Nicholas Lansman: I will kick off by saying that as far as the industry is concerned, from our initial look at the Bill it is clear that it does extend and does not continue with the existing maintenance of what is required to retain data. So the Government are looking to increase their capability in a way that will cause a great impact on the industry.

Malcolm Hutty: I would break the question down slightly. The aspect concerning whether the issues need to be addressed touches on the appropriate balance—the place to draw the line—between the privacy of the individual and the interests of law enforcement and public authorities in acquiring data to use to support their legitimate missions. We really do not want to get ourselves into expressing a value judgment on where that line should be drawn. We understand that this data is extremely useful for legitimate law enforcement purposes, and that is right. At the same time, data is also intrusive and there is a legitimate privacy interest. Where to draw that line is an important thing for Parliament to decide. We do not really wish to express a view on where it is appropriate to do that. However, as an industry, we feel that we have a responsibility to provide the benefit of our technical understanding of the likely impact of this on that balance. So when we hear the Government telling you, as they have told us, that this is essentially just a minor technical update to bring the current powers into line with the change in technology, we feel that it is incumbent on us to explain our view that it goes very substantially beyond the existing impact in terms of where that line is drawn. Whether or not you should authorise that—whether it is justified by the security need—it is a matter for you. But we will say that this data goes far beyond what has been done in the past. I watched yesterday’s exchanges, courtesy of the webcast, and I would like to make a few comments on the exchanges with Mr Ellis in particular on this point. If it were simply the case that the volume of data but not its nature were changing—the fact that there was more being collected, but it was now a reduced proportion of the total—the relevant thing would be that it was a lower proportion of the total. However, what we are looking at under these proposals is not merely changing the volume of data that is collected but also the nature and character of that data. For example, when the Interception of Communications Act was dreamt up, which set the framework and the basic idea of the separation of interception of communications data that was followed in RIPA, we were essentially talking about, on the one hand, the content of communications, which is a window on a man’s soul, and on the other, data such as an itemised phone bill, which is just a business record. But now, as regards communications data, if you simply look at just web accesses you are seeing stuff which, even if it is not content, is very much more likely to tell you a lot about the nature of the person. There are therefore three things to consider. Stop me if I am going too much into this, but there are three different types of communications data that I would suggest one might look at. One is material that shows information about the associations between people—for example, it shows that you, Lords, Ladies and gentlemen, are all related to each other and may indicate that my Lord Chairman is the ringleader, because your office sends out messages that are all clustered tightly together and therefore identify that you are saying, “This is the time when we will meet”, for example. That is association information. But then there is information that identifies stuff about the nature and characteristics of persons themselves. That might include, for example, the fact that, Mr Mosley, you read ConservativeHome and the Daily Telegraph, or
that you, Mr Brown, may read the Guardian. That may signify something about your respective political inclinations. I am just making this up, but say, Mr Brown, you were looking at the GMB’s website, and not the public website but a private site, without knowing what it is, it might nevertheless suggest that there was some ongoing relationship between you and the GMB—possibly that you were doing a bit of political consulting and so forth. Baroness Cohen said before that she shopped at Ocado. You asked previously whether the contents of your shopping basket would be included—and indeed they are not. But the mere fact that you shop at Ocado might suggest something about your socioeconomic category, and combining that with other communications data might tend to corroborate that. However, if we were to go to something much more intrusive that may give much greater concern, such as geolocation information—the location of where a communication is made from—if it is made from a fixed location, that means, “Oh well, this is just his home address”, or something like that. However, in the world of smartphones, where that phone is asking maybe every five minutes for an update on whether you have a new e-mail or a weather application, one is getting as communications data events a track of where you are from moment to moment. That is not something that is normally tracked by the service provider and is certainly not centralised and made available in a way that would be meaningful, but it seems to be within the spirit of the draft Bill that that is the sort of thing that could be done. If it were the case that communications data were to suggest that a member of this committee or someone, while they went home immediately to their constituency on a Thursday night but on a Wednesday night went out for dinner in the West End and then stayed overnight at an address where the fixed line was not registered in their name or the name of their spouse but in someone else’s name, one might well think that that kind of information was highly intrusive.

The Chairman: Thank you, Mr Hutty. You went on a wee bit at length there, but you nevertheless opened up an interesting can of worms that we will all want to explore. We will not leave this subject, but I want to hear if Mr Wales has anything to say, first to the opening question, and we will then come back to the issue of the 25% gap and the content of data.

Jimmy Wales: I just have one small addition to what has been said before. Mr Hutty indicated that as a representative of an industry association he did not want to take a position on where these lines should be drawn. As I am speaking today in my personal capacity, I have rather strong views on this. We are talking about fundamental issues of individual rights—human rights of privacy. Whatever we may do here, we should attempt to do it—to the extent that these issues need to be addressed from a law enforcement perspective—with the least possible impact on ordinary people who are not committing crimes and are simply going about their lives. The separation—and I am sure that we will get into this later—between the content and the addressing of information is much more difficult to define, and I would argue that it is essentially impossible. To find out a great deal about someone, you need only to know which blogs they are reading or which Wikipedia articles they are reading. I consider that to be a very personal question. People may be reading it for all kinds of personal reasons that do not implicate them in any criminal way. It is very difficult to argue that we should be tracking that sort of information on ordinary citizens who have no inclination of any kind to be involved in a crime.

The Chairman: Thank you very much. Mr Hutty talked about the 25% gap—I am not going to ask a question on it; I will just ask colleagues to pile in. I thank both ISPA and LINX for your
excellent, detailed and absolutely fascinating written brief. You have pulled no punches and you have been critical of many aspects of the Bill. My colleagues may wish to continue to question Mr Hutty and Mr Lansman on the 25% gap, which the Home Office alleges, and Mr Hutty’s comment that there is a huge volume of new information.

Q511 Lord Strasburger: We have heard repeatedly about the 25% capability gap between what the public authorities, principally the police and the security agencies, would like to get their hands on and what they can get their hands on. Does that mean anything to you? Do you recognise that 25% gap?

Nicholas Lansman: The figures that they have drawn up are obvious best guesses. We do not know how much data will be required to be collected because there is not a lot of clear information.

Lord Strasburger: This is said to be a current gap.

Nicholas Lansman: I still think it is a best-guess estimate. When we look to the future in terms of communication services and the data that will be collected, it could be vastly more. The important point is to understand better the meaning of the data that they want to collect and what it will be used for. That is the bit that, as an industry, we do not quite understand.

Jimmy Wales: I believe that 25% is a number made up out of thin air. I do not think that it has a basis of any kind. It is a rough estimate of something that is undefined. I do not see how we can even respond to a number like that.

Malcolm Hutty: I would like to ask: 25% of what? Is it 25% of all data or 25% of the data that we need? Is it 25% of something else? I do not understand what the 25% figure is.

Lord Strasburger: It was put to us as 25% of the data that they would like to get their hands on from time to time but cannot.

Malcolm Hutty: I appreciate that. However, I watched all the sessions and have had private meetings with officials seeking to understand this point and I remain confused about it. I do not wish to use the sort of language that Mr Wales just used about thin air but, frankly, I do not know how that figure was arrived at or could be arrived at.

Lord Armstrong of Ilminster: The impression I formed was that it was 25% of the accountable information that they got in the old days when all you were looking at was telephone communications and occasional interception of the mail.

Malcolm Hutty: But all that information is available under existing legislation.

Lord Armstrong of Ilminster: However, because of the enormous spread of telecommunications, they are in fact talking about a 25% loss of a much larger figure. I am not sure quite what meaning it has because I am not sure of what the larger figure is.

Jimmy Wales: This is essentially a less inflammatory way of saying what I was trying to say. If we are talking about new forms of data, such as your exact physical location every five minutes, it is an apples and oranges comparison. We cannot say that it is 25% more data. It is not just about the amount of data because the kind of data is so significantly different. It is very difficult to place a meaning on a numerical estimate like that.

Q512 Lord Strasburger: LINX’s written submission raised concerns about the requirement for companies to collect third-party information and third-party communications data. Do you all share those concerns about third-party communications data?
Nicholas Lansman: As far as ISPA is concerned, there is a great concern, which is largely down to the lack of knowledge that we have of the intention behind the Government on this. Third-party data is potentially an enormous amount of data. If it has to be collected by UK CSPs, that will impact on the industry, potentially in a very important way. It could be in terms of cost or driving down innovation, or just in terms of confusion for companies over knowing what they have to keep and what they do not have to keep. More information is needed before we can make clear statements and answers as to the effects.

Jimmy Wales: Yes, from our perspective at Wikipedia, this is a concern that we would have. It is important to understand how trivially easy it is for people to evade this sort of thing. We do not have servers in the UK. We would be highly disinclined to collect more data than we do, which is very little, for a variety of reasons, including our views on freedom of expression and human rights, and what people are reading. But if we find that UK ISPs are mandated to keep track of every web page that someone reads on Wikipedia, I am almost certain—I should not speak for our technical staff—that we would immediately move to a default of encrypting all the connections to the UK so that the local ISP would be able to see only that you are speaking to Wikipedia and not what you are reading. That kind of response is not difficult for us to do. We do not do it today because there does not seem to be any dramatic need for it or any dramatic threat to our customers. But I think that we would do that—absolutely.

Nicholas Lansman: Some of the information in our evidence suggested that this Bill would have the potential to chill innovation. Here, we have heard the example of Wikipedia potentially being willing to encrypt and to withdraw service in the UK. The question you have to ask yourselves is, "What will be the effect on other companies coming to and investing in Britain or trying to start new innovative businesses in Britain?". That is some of the fear that ISPA has: without the knowledge of what this Bill means, potentially, it could have quite a damaging effect on future innovation in the industry. Ultimately, that underlines and underpins a great deal of innovation and growth in the economy, which would affect financial services, manufacturing and all parts of industry that are now underpinned by the internet industry.

Malcolm Hutty: I would say that this cuts both ways. The inverse is also true. At around Christmas or thereabouts, we were led to believe that what was being considered by the communications data team at the Home Office was not to be focused on the collection of third-party data, probes in the network and big database search facilities. Instead, the focus was to be very much on seeking co-operation with the top providers which had the data for legitimate law enforcement requests. At the time that that was our understanding; we had a very different view of this. The criticisms that we make and the concerns that we raise regarding third-party communications data cut both ways. If you did not require that third-party access and were not building an enormous profiling engine that involved so many challenges—whether they concern privacy, technical feasibility or the effect on innovation—but instead focus on that aspect of the Bill that is about getting such co-operation as one is able to within the laws under which the over-the-top providers operate for legitimate law cooperation in the public interest, we would not have written the kind of submission that we have written today.

Q513 Lord Strasburger: What is the effect of encryption on retention of this third-party data? Presumably, if the data is encrypted, you would not be able to differentiate between
content and communications data, so if you were to retain it all would you not be at risk of retaining content?

Jimmy Wales: Just to clarify, if I am a UK-based bad guy and I think that I have heard that the Government are snooping on everything, what I would do immediately is open an e-mail account trivially—from any of thousands of free e-mail account providers around the world, and by default the communication for e-mail is encrypted—so that the only thing that you would be able to see from the UK service provider is simply that I am talking to that particular e-mail service. You could not see the content of the communications at all, because it would all be encrypted. If you saved that data, I suppose you could try to crack the encryption and so forth, but that is non-trivial to say the least.

Q514 Lord Strasburger: What is your understanding of what the requirement of the Home Office is for the retention of encrypted data? Would you be required to retain it or not?

Malcolm Hutty: We do not fully understand that. I cannot give you a direct answer, I am afraid.

Q515 Lord Strasburger: Is this requirement to retain third-party information likely to encourage more and more information to be encrypted? Mr Wales has already answered that.

Jimmy Wales: Yes, definitely. In fact, this is a broader trend in the industry for lots of reasons. Facebook is an example. These days, it offers encrypted connections for people for perfectly valid reasons of security. If you are using Facebook on an open wi-fi network, it was discovered a couple of years ago that people could snoop in, copy your session and view your Facebook page. As a response to that, more and more providers are encrypting connections. It is becoming less expensive to do that, and there are certainly good, sane and rational security reasons for doing it, so that people along the way cannot sniff your communications. That is an ongoing trend which will continue and be pushed forward—the demand for that kind of thing—by laws such as this.

Nicholas Lansman: You can see this as a trade-off, because the very fact that you can encrypt is very good for stopping fraud and making sure that banking communications and transactions are safe. But at the same time, it does make it harder for law enforcement to access this sort of information. Encryption is a very good thing for the customer and for business, but it does have the side-effect that it of course makes it harder to look at—

Malcolm Hutty: Well, to look at information that is passing over the wire. It makes it hard to do third-party data access but I go back to what I was saying before about our previous hopes that the main focus would be on the over-the-top provider, and actually asking them. There may be an encrypted channel between the user and that provider, but once it has reached the provider it is no longer encrypted and they have access and could co-operate, to the extent that they are able, within the regulatory regime that they operate under. As I say, the Home Office continually tells us that the main focus is there, but that is not what we see in the Bill.

Q516 Lord Strasburger: Mr Wales, in particular, how do you see any change arising in the behaviour of internet users if the Bill were enacted?

Jimmy Wales: Well, I think that you will encourage people to use services that are not based in the UK. One of the biggest impacts that we should be concerned about is: what does this do to the UK start-up industry, as the costs are substantial even though the Bill contemplates
compensating for those costs? I can tell you from my own experience, in the very early days of Wikipedia, we were growing very quickly. We actually stopped logging all accesses for quite a long time, simply because we could not afford the server space to keep up with them. We certainly did not have the resources to have a full audit of our security system in order to be compensated by the UK Government. We just had no resources even to think about that sort of thing. This is quite natural in the days of a start-up. So we are going to have two things. We are going to have consumers who think, “Gee, I’ve heard that the Government can snoop on my e-mail account if I don’t get one from the US”; and potential investors and entrepreneurs here in the UK will be faced with quite a burden of dealing with complex regulations to store data that they otherwise would not store for business purposes.

**Q517 Dr Huppert:** Can I just press briefly on this issue about encryption, because I think it is critical to the success of the Home Office scheme? As I understand it, the Home Office scheme is that if people will give them the data from outside, that is great; if not, they will require CSPs to install black boxes to suck it out. As we have already heard, it will very quickly become encrypted, so it could only work if there was a way of breaking the encryption. I would be very grateful for a professional assessment from each of you. I have heard about things to do with fake certificates, man-in-the-middle attacks and various other options. How plausible is it, on that sort of scale, to break any of these encryption technologies?

**Jimmy Wales:** It all depends on how dirty you want to play. Certainly, the UK Government could engage in a wholesale systematic effort to do man-in-the-middle attacks to capture people’s internet traffic. This is the sort of black-hat hacking. It does not sound like something that a civilised democracy would want to be involved with necessarily; it is more like what I would expect from the Iranians or the Chinese, frankly. Is it possible? It is not easy, and it would be detected immediately. That is the thing: this is not something that you could do at any scale without the internet community noticing it and sounding the alarm. People check these kinds of certificates; things do get exposed. It is mind-boggling to conceive of even thinking that this is a rational public policy.

**Malcolm Hutty:** From a commercial perspective, it is that issue—that it would be detected—that would probably be the thing. I doubt in all seriousness that the Home Office is contemplating man-in-the-middle attack-type things such as have been speculated about, because it would be detected, as you say. The impact on confidence in business communications of real value would have to be weighed against the value for law enforcement. I am sure that it would be concluded that the harm done to the economic interests of the UK outweighed any potential benefit.

**Q518 Dr Huppert:** So the consequence of what you are saying is that, if this Bill were to go through essentially as it is, that section that deals with making CSPs collect transiting data would very quickly become completely useless because all the data you were going to collect becomes encrypted and then you cannot get any of it anyway. Is that right?

**Jimmy Wales:** That is my belief. It is important to understand that, often when we speak about encryption, man-in-the-middle attacks and that sort of thing, it is quite easy to imagine, “Oh well, a few people could evade them but, frankly, your run-of-the-mill terrorist, paedophile et cetera is not that technologically sophisticated so we still think we could get a lot of it”. If we think that way, it is absolutely true. People could start using complex encryption
tools; it might go up a little bit, but it would not be the main factor. The main factor for me is as simple as, “I’m not going to talk about things on Facebook or Google or the places that I know that the big companies—the responsible companies—are going to co-operate with law enforcement; I am just going to use a free e-mail provider in a country that’s not the UK”. It is quite trivial to get round it.

Malcolm Hutty: I have a different answer to that question, Dr Huppert. I do not think that it does completely undermine it. It prevents one element of what is being sought here from being recovered. Mr Wales’s reply there relates to things like the messaging that happens on Facebook and the messaging that happens on Gmail, which it would prevent. But if you go back to my opening statement about the different kinds of data, we would still know that you were shopping at Ocado even though your communications with Ocado were encrypted. We would still know that you read ConservativeHome and the Daily Telegraph and that Mr Brown read the Guardian.

Q519 Dr Huppert: But we know that now, do we not?

Malcolm Hutty: Well, no. That is not something that is collected; it is not something that is made available. E-mail and telephony records are collected. Certainly, the tracking of people around the city—their geolocation information—would not be prevented by encryption, because which cell site your smartphone connects to is known by the network operator, so no encryption there is going to defend against that kind of thing. Certain types of communications data would still be very much available, and they may very much go to many of the things that I opened on at the beginning. What it would impact on is the ability to track the more traditional messaging through the new technical means such as Google Mail and so forth.

Q520 Baroness Cohen of Pimlico: I have a question for Mr Wales. Is encryption very expensive? You said that you would, if necessary, encrypt Wikipedia communications; have you had a shot at costing that? This would help my thinking. Is it very expensive or very cheap?

Jimmy Wales: Very cheap. I have not formed a precise estimate, but I could ask my staff and get back to you. It is not expensive any more. There was a time when doing good encryption on the fly was difficult and expensive but servers are very powerful now. When I and millions of people use Facebook, every page is encrypted. It is just an option you turn on in Facebook, which does not cost anything. It costs Facebook something but nothing material.

Q521 Baroness Cohen of Pimlico: It is not an inhibition?

Jimmy Wales: It is not an inhibition, no. In fact, many kinds of communications are already by default encrypted. For example, when you download your e-mail from Google, that connection will typically, by default, already be encrypted. E-commerce sites are encrypted by default in things like that. It is not a big deal any more.

Q522 The Chairman: Suppose that I sign up to Facebook and tick the box for encryption, and my messages are encrypted. Presumably it uses a standard encryption code or a key, so that if the Government crack one of them, they can crack the next couple of million—or is every single message using a different code or page?
Jimmy Wales: It is closer to the latter. It is not as though you just need the one password for Facebook encryption. Every session would be encrypted with a certain key that is generated. I just want to point out that Facebook is probably not the best example. Facebook, for its own business and cultural reasons, already collects massive amounts of data and saves it for ever. Consumers are deeply concerned about that. And, of course, Facebook is a responsible company, with operations in the UK, so if law enforcement wants to find out everything you have done on Facebook, it can just get a court order already; that is quite simple. It is not clear to me that the Bill would impact on Facebook very much. Of course, I do not know what the people from Facebook may have to say about that.

Malcolm Hutty: Lord Chairman, if you need details on that last point, I suggest you direct them to Professor Anderson, who you have already heard from and who is a world authority on the subject.

The Chairman: We may wish to speak to him again. Could we move on to communications data and separating it from content data, Lord Armstrong?

Q523 Lord Armstrong of Ilminster: You touched earlier on the difference between communications data and content. It is important in the Bill, perhaps not least because access to communications data can be authorised without intervention by a judge or the Secretary of State, whereas interception of content requires a warrant. I think we have been forming the impression from what you said that the border between data and communication is very porous. You talked about the accumulation of data that told you a lot. The other matter is technical. Is it technically possible to separate communications data and content in your world?

Malcolm Hutty: To some extent, yes. There will be edge cases where it becomes increasingly technically difficult. There will be further edge cases, at the extreme, where it is conceptually difficult. For example, if I were to send you an e-mail, the fact that the message was to you is communications data and what I write to you is content. If, within that e-mail, I say, “Please pass this message on to my Lord Chairman”, is the fact that that message is included within it communications data because you are going to be doing it? If it is written in prose, does that mean it is content; but if it is written in a manner that makes it easy for you just to click a button and do what I have just said, does that suddenly turn it into communications data? At the edges, there will be difficulties of understanding. Furthermore, the simple technical difficulty of having probes within the network that analyse network traffic—third-party network traffic that you do not know yourself and do not understand, but where you have configured that box in a manner that seeks to pick out those bits that are communications data, and discard the content—depends on the idea that we understand the nature of that traffic and can identify those bits of it that are communications data, even though they are intended for somebody else. For example, they can scan a web-page transmission from Google Mail to the user and pick out of that web page that it is really just a web page that performs the function of an e-mail, that within that e-mail there is a line that is a to-line or a from-line or so forth, and that that is communications data and pick it out. To be able to understand that that web page is really an e-mail, and that this element—this particular e-mail address within it—is a communications data element, whereas this other e-mail address, which is maybe in my signature in my e-mail, is not, and to be able to distinguish between those two, and to continue to be able to do that every time the provider, such as the website concerned, changes the design of their web page, those boxes need to be reconfigured so as to be able to do all that
again. Then, you may need to extend that into other protocols, for example beyond web and e-mail. The Home Office’s consultation paper spoke about being able to understand when people were chatting to each other in computer games. There you do not have anything like the same simplicity, even in the complicated question that I have just described. There you have a computer game client that is written by a private company and the game server—which is written by the same private company, using its own protocol that is made up and may be changed from day to day by that private company—and you are trying to guess which elements of it amount to communications data and programme that box so as to be able to do that. So there is an element to your question which is whether we are going to be able to do that in practice. That is going to be an enormous technical challenge, to put it at its mildest.

Q524 The Chairman: May I just interrupt there? Could you clarify? You said “games”, so can kids or people playing on an Xbox or Nintendo communicate?
Malcolm Hutty: Yes.
The Chairman: And you can send messages through Xbox and Nintendo?
Malcolm Hutty: That is right, yes.
The Chairman: Good Lord. Sorry, Lord Armstrong.
Malcolm Hutty: I might also say that the most popular demographic for playing such games is no longer children.
The Chairman: I apologise to the 10 million people I have offended.
Malcolm Hutty: It goes to the relevance. Is this just something at the margin? Let us face it—we are not really going to be interested in a law enforcement need to look at what children are saying to each other. Actually, we are talking about young men, of maybe 18 to 35, whose communications might be of interest. But it will be extremely challenging to be able to acquire them in the manner envisaged by the Bill.

Q525 The Chairman: So you are suggesting that potential bad guys, al-Qaeda in future, could use things such as Nintendo or Xbox that would not be caught by this Bill?
Malcolm Hutty: They would be caught by the Bill, in terms of the intention. That is why the Bill is so broad as to seek to get anything, including mere computer games. But it is going to be very difficult to deliver that.
The Chairman: Yes, but unless the Home Office were to serve the orders on them to comply and install the DPI boxes and so on, they might not be caught that way.
Malcolm Hutty: Yes, the Home Office would have to decide that it was going to set us that technical challenge.
The Chairman: Sorry about that. Lord Strasburger? No. Moving on, Baroness Cohen with question six?
Baroness Cohen of Pimlico: I think we just missed question five, but I think we have the answer.
The Chairman: My apologies.

Q526 Baroness Cohen of Pimlico: My question was to ask generally whether you think that it will damage relationships with service users, for them to know that companies are retaining and sometimes disclosing stuff to the Home Office. Do we think that the extension of this Bill will make people very leery?
Malcolm Hutty: I think that it would very much impact on the nature of the relationship between the service provider and the customer. There is something in the precise phrasing of this question that signals to me that you are asking whether I think it would be better if we kept it secret.

Q527 Baroness Cohen of Pimlico: I was going to ask it the other way around: would it be better if you made it public?

Malcolm Hutty: I am certainly not sure that it is really possible to keep it entirely secret. If you think that the customer might be upset by something that you are doing so you try to keep it secret from them and then it comes out in the open, they are even more upset. It might not be a wise public relations strategy to go down that route. It would of course be a matter for individual businesses to consider, if the possibility is available to them, unless you decide to make it very open. The alternative route would be as you say: to bring things out into the open; to say that there is a legitimate need for so much and no further, and we will have that with a democratic debate, a justification and parliamentary approval, and then providers simply comply with the law. That is fine, in so far as it goes, but it does impact on the nature of the relationship with the provider. The providers have always provided support for communications data, but with the nature of the material that we spoke about earlier—phone call records and so forth—you are essentially talking about a business document. The nature of the co-operation that is given there can be characterised as that of any responsible citizen who, if they come into possession of something that is necessary for an actual law enforcement investigation, should of course help with that. It is just like being the witness to a crime: you tell the police what you saw. Similarly, if you have got this communications data, you hand it over in that fashion. But you do not necessarily go out looking for things that you do not already have a business need for, which you do not have for your own proper purposes in serving the customer. That is more like joining the police on a stakeout. That is not what most ordinary citizens do, even corporate citizens. It is not entirely without precedent. Communications providers have always supported lawful intercept capability. That is going beyond just, “Something happened and therefore we will co-operate”. That is providing a specific design service to support law enforcement needs that is very proactive. But the lawful intercept capability is a very limited thing by comparison to this. Most people are not going to have their phone tapped.

Baroness Cohen of Pimlico: I need to shift the focus of my question a little. Mr Wales, you come at this from a slightly different angle. Presumably you feel that it would damage your relationship with customers if the Home Office suddenly arrived on your doorstep—not that it would ever have the power to do that directly. That is why you would encrypt Wikipedia.

Jimmy Wales: Yes.

Q528 Baroness Cohen of Pimlico: Is this partly a moral decision, partly a commercial decision?

Jimmy Wales: Well, in our case, as we are a non-profit charity, we do not normally think about commercial things. We do know that our user base is quite passionate about freedom of expression, privacy and this sort of thing so, as a charity, I do not think that it would hurt us commercially: we would probably get donations from people who feel that we have made a courageous moral stand. But, in general, I think that one of the things that we really put forward and try to make people feel comfortable about is that what you read, what you want
to learn about, is very personal and important. We do not give out that data lightly. In fact, we
do not keep very much of that data at all. We keep extensive data on when people are editing
Wikipedia, of course, because we have to deal with bad behaviour and things like that. And we
co-operate with law enforcement. We will always obey, of course, a US court order, but we
will also co-operate with law enforcement overseas if it is naturally and obviously the sensible
thing to do. We feel that if you have a judge who has ordered you to keep track of something,
or who has ordered a specific inquiry on a specific thing, it is very different from—and this is
where I get to the answer to your question—a broad programme of storing large amounts of
data which we would not otherwise store on innocent people. We think that that undermines
the humanity of what we are doing. We are writing a free encyclopaedia and giving it the
world. It is our gift to you; it is not our way of surveilling you. You should feel comfortable
when you are reading Wikipedia that it is your own personal business. That is the way that we
come at it.

Q529 Baroness Cohen of Pimlico: Can I have a go at a slightly more technical question?
You said that you thought that the need to encrypt would inhibit innovation, if people had to
think about that. Do you think that it would impede innovators such as yourself if you had
had to think about keeping data for law enforcement authorities? That is a technical question,
not a moral question.

Jimmy Wales: Yes. From a purely technical and business-process point of view, in order to be
successful as a start-up you really have to be incredibly passionately focused on what it is that
you are building, what it is that the customer wants, what it is that is going to be useful and
practical and which people will enjoy using. Many of the most successful start-ups began with
a team of two people, five people or one person. To impose on them a separate requirement to
keep data that they would not otherwise keep, but also keep it under conditions of security
which are, as a moral and legal responsibility, quite onerous, and to design their entire system
around that—if they are not being compensated for it, it is obviously a huge barrier. But even
if they are compensated—if we think of any realistic programme of government
compensation—we will have to guard against people who set up businesses simply to milk the
system by gathering data on people: “And now you’ve got to pay me to take care of the data”.
That means that I will have to interact with a set of regulations and a set of audits of my
processes. It is hard for me to conceive of how you could do that without having a team of
people working on it. In a small start-up it is not really conceivable to think about how you
could do that. It is much easier to move to Germany.

Malcolm Hutty: That impact is not limited to small start-ups. You can speak to a large
company and they can have a whole department devoted to this and their jobs depend on
implementing all this stuff and everything seems great as a steady state. When you take on
board an obligation like that, you are not simply taking on board the duty to do it now, but
also that any future changes that you make—any developments that you make to respond to,
maybe, these small start-ups that are trying to eat your lunch—must also be compatible.
Everything you must do must have this new thing built into it before you can get started. If
you wonder why small start-ups sometimes seem more nimble and larger companies
sometimes seem a bit slower to act, it is because large companies have so much which
anything new they do must fit in with. When you start layering on incredibly complex and
burdensome technical requirements, even if they are fully compensated for the ongoing process, it limits their ability to react to market demands.

Q530 The Chairman: Mr Lansman, you represent over 200 companies large and small. Is that your view of the impact on innovation cost as well?

Nicholas Lansman: Yes it is. It is a very fair point that both my colleagues have made, about the effect that, for different reasons, will apply to very large companies and the smallest ISPs. ISPA is made up of the top 10 large communications service providers, but equally has a large number of smaller companies who provide business-to-business services to a large number of British businesses, SMEs and upwards. For different reasons, they will have concerns about this, waiting for the notice to come, which it may or may not. It may be that the Home Office is focusing on the larger providers at the start. If you are running a business and you think that you maybe have something coming around the corner that says that you now have to comply with this law, that is a worry. If you are designing products and services for your business customers, your focus will then be on thinking about an obligation to retain data rather than providing efficient, innovative, cost-effective and speedy services. That, I think, is a distraction.

Jimmy Wales: In this context it is important to focus for a moment on the numbers that we are talking about: £1.8 billion over 10 years, so £180 million per year, which I think is an underestimate. Maybe I am just a bit cynical about government estimates of numbers but, as we all know, these things tend to go up. I looked up the numbers of the members of the British venture capital association. Their total investment in the internet industry in the UK in 2011 was £37 million. When we think about the magnitude of what we are asking—an £180 million expenditure on building a system for collecting data—how does that compare to the total investment in innovation in the UK? I should point out that the BVCA represents the venture capital industry. There is a lot more venture investment than that—angel investors and things like that—so I am not suggesting that this is the whole of the investment. But if we start to think about the magnitude of what we are doing as a society, even a small amount of money has generated a lot of excitement about the silicon roundabout and the Shoreditch start-up scene. To me, it boggles the mind to think that we would spend this much money in this way, when we all feel that investing in start-ups is something that we should be doing more of.

Q531 Stephen Mosley: Within LINX’s submission, there was a big section on the filtering arrangements, which you call the profiling engine. You have talked about it in quite a bit of detail earlier, Mr Hutty, so I ask Mr Lansman and Mr Wales what they think about the filtering arrangements. Do you think that they impinge on an individual’s privacy?

Nicholas Lansman: I think the first thing to say is that we do not know a lot about it. We know it is called a filter. We know that in LINX’s submission they have called it a profiling engine. People on the Committee have called it a search engine. I think that, knowing more about what it might do, when the Government present it as something quite innocuous and say that the object is to stop the Government from getting too much data that it should not look at, it could of course be used the other way. The fear, without the knowledge of what it will precisely do, will be that it will actually look at data from different people and be able to make, I suppose, judgment calls. That is, I think, of concern not just to ISPA and us but to the average person in the street.
Jimmy Wales: One of the concerns that people have had in the past is about the notion of a centralised database. This scheme is in part supposed to allay our concerns about that because all of the data will be held in individual databases. This raises other questions, because the more individual service providers have databases, the more chances there are that somebody is going to be sloppy and let loose some data. This search-engine profiling point, the filtering, becomes quite an interesting point of attack for anyone who is trying to gather information about an individual. If we are gathering data willy-nilly, indiscriminately, on everyone, not just criminal suspects, suddenly we have a system where someone could make a request and get huge amounts of information about an individual. That seems like something that it would be very risky to have. Whether it is technologically stored in a single database or is some kind of interface to a lot of different databases is a concern. As Mr Lansman said, we do not really know enough about it to fully understand it. I think I am in the wrong room to bring up tabloid newspapers—that is the Leveson inquiry—but we have seen quite unfortunate circumstances of people paying for information from the police. How much more tempting is it, rather than asking the cop which celebrity went into this restaurant, to say, “I would like all of Rupert Murdoch’s e-mails, please”, or just the communications data on them? To me, it seems like a very dangerous thing to have available. That does not mean that we cannot keep it secure, but it is a serious concern.

Q532 Stephen Mosley: Talking to other witnesses, we have heard that there is some concern that there might not be a direct tie-in between the data held by yourselves or the companies you represent and the eventual evidence that the police, or whoever it is, actually use in court. Do you share concerns about the transparency of the filter results and whether those results will then actually be able to be used as evidence in the future?

Nicholas Lansman: That is one point that ISPA has made—the more that you interfere with databases, query and mess around with them, there is a danger that the data becomes less evidential as regards the level of quality that the court would be prepared to accept. I think that that is a risk. Having said that, it may be that law enforcement is looking at this to provide intelligence that may well be of very important use in tracking crime. It is the debate that we mentioned earlier. It is: what is proportionate in terms of inquiry of the data to solve some very bad crimes? I do not think that it is for the industry to ask these questions, but it is for Parliament to properly scrutinise this and ask the questions, “Is this level of filtering appropriate?” and “Is it what we need to track down appropriate crimes?” If it is, then fair enough. But if it is too intrusive, that is then a decision that Parliament should be taking, not the industry.

Q533 Stephen Mosley: The draft Bill gives the Secretary of State powers to transfer the functions of the filter to a third party. Is it a designated public authority? The draft Bill is not too clear on that. Do you think that this would create a more arm’s-length approach that might be advantageous or might it be a disadvantage and create problems?

Nicholas Lansman: My colleagues may chip in here, but the initial point that we have made is that abrogating this responsibility to a public authority is not always a good thing. Again, there should be some sort of parliamentary oversight of this process. Just handing over a lot of power to another public authority is not necessarily a solution.
**Malcolm Hutty:** The Home Office is not an investigating agency but a central government department. I really would not envisage it implementing or running this facility, this profiling engine, itself. Some agency would be tasked with that or created for the purpose, and you have mechanisms in the Bill to handle that. I think you want to divide out the different things that need to be done here. There needs to be creation of policy. There needs to be operational use of this facility, if it is to exist, and there needs to be some oversight of it to ensure compliance with policy, to discover non-compliance and to correct it. There are three different functions. The operational side should be separate from at least the other two. There are models that you could consider that put the policy-setting side and the compliance-oversight side together—that is how the Financial Services Authority works, for example—or separately, which is what we have under RIPA. The Home Secretary currently sets policy and the Interception of Communications Commissioner has the oversight function. You can put those two functions together or take them apart, but you really have to have the operational side separate from either of them.

**Q534 Stephen Mosley:** Would you be able to suggest what sort of authority, or which authority, should do that?

**Malcolm Hutty:** No, it is not for us to say. This is essentially about how you organise the police law enforcement in the round, and the intelligence community, all being served by this function—and that is beyond our scope.

**Q535 The Chairman:** Others have suggested that leaving the setting of the filter’s parameters or its programming to GCHQ would be inappropriate in a democracy, given that GCHQ comes from a military background—quite rightly—spying on overseas dangerous characters and military threats, and that responsibility would be better placed with the police, for example, who would be slightly more, or a lot more, accountable to Parliament and local democracy. Do you have a view on that?

**Malcolm Hutty:** If you want any accountability in this, you need to set a framework for that accountability to take place, including some basic values judgments as to where lines are to be drawn. We do not seem to have in the draft Bill a mechanism for that to take place, which is one of the reasons why in the answer to your question on that subject we are critical of the level of parliamentary scrutiny that is proposed under the Bill. It is not so much a question of who does it but of what the frameworks are. Who is going to oversee it? What are their powers going to be? In which areas should rules be written? What kinds of rules are to be required? It should be something that gives a parliamentary steer on this issue of what is to be considered proportionate.

**Q536 The Chairman:** It is quite unusual to hear an organisation representing 450 private companies wanting more parliamentary scrutiny or interference, but I picked that up from your written text also. What about the Interception of Communications Commissioner’s office? I think you have been reasonably critical of its role so far. How do you see its role in the future? How would you change it to satisfy the demands for scrutiny that you have suggested?

**Malcolm Hutty:** As we said in our material, the role of the Interception of Communications Commissioner is not entirely clear but can be inferred somewhat from the way that that function has been carried out, and it appears from the nature of the reports that have been
written to have been focused largely not on the broader questions that I posed back to you but instead on a narrower question of whether we can be assured that there has been no widespread misuse of RIPA powers. That is a perfectly proper thing for there to be oversight of, but it does not necessarily extend to the full range of oversight of covert investigation policy that you might want.

The Chairman: So you are suggesting that the commissioner looks to see whether this is in compliance with the current law—yes it is—not whether the current law is now being exceeded by technology.

Malcolm Hutty: Indeed. Some of the questions about whether it is justified to ask for richer kinds of data and whether it is appropriate that we should be treating geolocation data as mere communications data, rather than content, are the sorts of things that the Information Commissioner has a habit of raising—not in this area but by analogy. The Information Commissioner has a habit of raising questions about the general framework of data protection and of stimulating a debate in Parliament on these topics. I have never seen the Interception of Communications Commissioner do any such thing in this area.

Q537 The Chairman: So would you advocate a new body or would you really beef up the interception commissioner’s role?

Malcolm Hutty: It would be going beyond my mandate to make a specific suggestion. I would simply point out that a good framework of regulation in this area which people can be confident in, and that actually delivers the legitimate law enforcement needs, has certain requirements that I have set out in some detail in our written response. They need to be met and are simply not present in the Bill; they are left for later.

Q538 The Chairman: One final point from me. As regards consultation requirements in the Bill, do you have a view on strengthening them before orders are placed on any of your companies?

Malcolm Hutty: The requirement to consult the company on technical matters and the ability to appeal the results of those discussions to the Technical Advisory Board is welcome—first, to ensure that things can actually be done at all; and secondly, to ensure that they can be done within the cost framework that is being discussed. That is essential. However, your question touches on something more broadly. Beyond the technical feasibility of implementing a specific requirement and the direct financial cost of doing that one thing, is that the full extent of the company’s interest in the matter? We would argue not and that we also have an interest in matters such as proportionality of the collection at all, because it impacts on the nature of the customer relationship. The broader financial question of unrecoverable costs, which I have gone into in some detail in our written evidence, goes beyond the scope of what you could discuss in the consultation and beyond what the TAB is allowed to consider. It is not therefore going to be open to our members in those consultations to say, “No, this is becoming too much of an overall burden for us”, “It is diverting us too much from our mission”, or, “Our users are fleeing to our foreign competitors because they do not want to use a service that is accessible in this way”. We are not going to be able to discuss any of those things in those consultations. The only time that we could discuss the issue is if detailed legislation needed to be brought forward. If secondary legislation were required to have much
more detail than is being set out in the Bill, we could then come to you and say, “This is having this impact and we should act on it.”

Q539 The Chairman: Are you aware of whether any of your members or you as organisations have raised these commercial and cost concerns, or the possible impact on innovation, with the business and industry department? There have been a lot of discussions with the Home Office. Have there been any with BIS or the e-mail and internet tsars?
Malcolm Hutty: Not at a high level.
Nicholas Lansman: To our knowledge, the answer is no. But, obviously, we are not privy to all the communications of our members directly with government departments.

Q540 The Chairman: So is it possible that BIS is just not aware of these concerns?
Nicholas Lansman: ISPA has had meetings with BIS. I am sure that it is aware of these concerns. We may need to redouble our efforts in meeting with it again.
Malcolm Hutty: We are not sure that there is political awareness of it within BIS.
Baroness Cohen of Pimlico: You mean, it said, “Yes, yes”.
Malcolm Hutty: We have routine contact with junior officials on a range of matters at which we disclose the things that are impacting us and what we are working on, particularly as regards international matters on which we have a strong history of co-operation. This has been raised so I could not say that there has not been any contact. But on the idea that this is being engaged with, in the broader sense the answer is no, even though strictly the answer is yes.
The Chairman: We will make inquiries and try to get to the bottom of it.

Q541 Lord Strasburger: The effect of this Bill would be to create a large number of databases distributed physically about the country. The effect of the filter possibly would be to make these logically into a central database. Does that have inherent risks of loss of data, intrusion or whatever?
Jimmy Wales: Yes.

Q542 Lord Strasburger: What are those risks?
Jimmy Wales: Any time that you require people to keep data, that digital data will be stored somewhere. It will be on a system that needs to be accessible. In particular, if the filtering system needs real-time access to the data, it will need to be accessible on the internet. There is always the chance—it happens with some regularity—that an ISP's servers are compromised and data is stolen. Even the perhaps most technologically advanced and security-conscious company, Google, pulled out of China because of a phishing attack by someone that compromised some of its servers. I do not know who, other than the Chinese Government, would be interested in the e-mails of Chinese democracy activists but that has never been proven. When even Google is vulnerable at times, although it is very good at this, we have to have some concerns about every small ISP, small start-up internet service and so forth. Keeping that data confidential is non-trivial. Servers are broken into all the time and there will be leaks of data for sure.
Malcolm Hutty: Risk is a function of impact as well as likelihood. In terms of likelihood, our industry has a very good record on protecting private data and its databases from technical attack. But nothing is ever perfect and sometimes problems happen but it is very rare. However, there are other mechanisms. Certainly, what concerns us more greatly than technical attack in terms of likelihood is the insider threat and the ability to compromise individuals who have legitimate access, and getting them to misuse that legitimate access. Frankly, we will wait to see what comes out of Leveson and Operation Elveden, which was directly related to that. I think that we might learn quite a lot from that. Certainly, that seems much more likely if the motivation is great enough. Looking at impact, you think, “How much would people want to get access to this? What could they do with it?” I do not think that it is appropriate for me in public to go into great detail about all the dreadful things that could be done. I skimmed over a couple in my written submission. If you would like some more information in a private briefing—perhaps if you have questions about whether what we are suggesting or hinting at here is realistic—we would be happy to get back to you.

The Chairman: We will probably take you up on that. If you have other information that you wish to send us and you wish to be kept confidential, we will respect that. We prefer to see it, hear it and read it, and keep it confidential, rather than not get it at all. If you would discuss that with officials afterwards, we would probably like to take you up on that.

Malcolm Hutty: I would like to hear what kind of thing you would like to have. Certainly, we will conduct that conversation about what would be most useful with officials.

Q543 The Chairman: Perhaps I may begin to conclude this. It has been a long session and we are very grateful to all of you. We have heard a lot of discussion on costs. I have read your brief and you comment that no government computer contract has ever come in under budget or on budget. We all understand that. Have any of your members shared with you their best estimates of what the costs may be, including any legal liability if it goes wrong? If I was one of Apple’s 12 million customers yesterday and found my data in the public domain, if I was an American probably I would be suing already for a couple of billion. Have your members made any estimate of the technical costs?

Nicholas Lansman: When we have had discussions at ISPA between members to try to answer this sort of question, the problem as regards costs is how long is a piece of string? We do not yet have enough information from the Government to know what they want stored, for how long or which types of data. It is very difficult to put a clear cost on it. My colleague also pointed to the fact that if you are designing future services, the opportunity costs of not focusing on your business and looking at potentially having down the line to store data is another cost that we cannot clearly put our finger on. A good example is, if we were asked to store third-party data from over-the-top services, such as Facebook and Google, the amount of data rockets and therefore the costs would increase. We also do not know what the future impact will be of greater data over the next, say, 10 years, which will also impact on costs. It is very difficult to give a very clear answer but, generally speaking, whatever the costs will be, it will probably be more.

Q544 The Chairman: My final question is: is RIPA fit for purpose in that the Government are now trying to collect a whole range of new information using the model of the 2000 Act and its definitions of “content”, “data”, “subscriber” and so on? If you were starting from
scratch, would you use RIPA as a model or would you try to invent new and better definitions?

_Malcolm Hutty_: If you are trying to provide a framework for efficient and effective covert investigation of electronic communications that also has a coherent and balanced approach to oversight and to establishing norms of proportionality and ensuring that they are complied with consistently, we do not think that the current definitions are well aligned to providing the hooks by which you might impose particular policy judgments, whatever they may be.

Q545  The Chairman: Is that the view of the majority of your members?

_Malcolm Hutty_: We believe that that is so and that this is the general consensus.

_Nicholas Lansman_: There are different definitions at the European Union level. Within the directive, slightly different definitions and meanings are used in European directives compared to in UK legislation, which is another issue to be dealt with.

_Malcolm Hutty_: We can manage with RIPA as it is when it relates only to the things that are required to be collected under the data retention regulations because there is a narrow, specified set of data types. But when you start extending it into some of the areas that we have talked about here, it simply does not provide the hooks to relate to the intrusiveness of the data.

Q546  The Chairman: Mr Lansman, is that your view as well?

_Nicholas Lansman_: Absolutely. The definition of “subscriber” a few years ago is very different from the subscriber details of, for example, Facebook, which might give a lot more information than just name and address.

_Jimmy Wales_: Or, indeed, a lot less information. When you think about a subscriber, one of the things mentioned concerns who is in control of a particular e-mail account. Google generally will not know that. I just created a new e-mail account to accept RSVPs for my upcoming wedding. I signed up for the account and did not give my real name, address or anything else. Why should I? Therefore, one of the questions that would come into my mind is that if Google is required to cough up the real name of a person controlling an e-mail account, that will have a significant impact on its ability to provide free e-mail accounts in the UK.

_Malcolm Hutty_: Under Clause 1, the Bill provides that the Secretary of State could require the collection of certain types of subscriber data at the point of account sign-up that is not collected at the moment. The basis of third-party collection is stuff that you do not already need. But if you apply that to the over-the-top provider at the account creation stage, you could say, “Please supply your passport number as well”. One of things that could go in the notice from the Secretary of State to the provider is that you must collect the passport numbers of people who sign up for your accounts. Essentially, that would make anonymous accounts or pseudo-anonymous accounts impossible.

_The Chairman_: I think that we have to stop there. I am very grateful to all of you. I am sorry that it has been a long session but we could go on for another couple of hours, questioning you and your colleagues previously. Once again, thank you for your written submissions. If you have any other private information to give us, we will follow up on that. Thank you all very much.
THURSDAY 6 SEPTEMBER 2012

Members present:

Lord Blencathra (Chairman)
Lord Armstrong of Ilminster
Baroness Cohen of Pimlico
Lord Faulks
Lord Jones
Lord Strasburger
Mr Nicholas Brown
Dr Julian Huppert
Stephen Mosley
Craig Whittaker
David Wright

Evidence heard in Private

Google [Sarah Hunter], Hotmail/Microsoft [Stephen Collins], and Yahoo! [Emma Ascroft] (QQ 547-600)

Examination of Witnesses

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!

The Chairman: Welcome. Thank you very much for coming this morning. We are grateful to you. This is a completely private session and I believe that our officials have discussed with you that we will take a transcript and then would like to discuss that with you as we hope that there might be parts of it that we are able to publish. We will be honour-bound not to do anything that would embarrass you or cause you difficulty. We want you to talk frankly to us. If you talk frankly, we can use that information to come to more sensible conclusions than if you do not spill the beans to us. We will respect your view if something is so sensitive that you do not want it out. We would prefer to have that information and not publish it than not have it at all. Perhaps a very brief word on who you are—Sarah, first, please.

Sarah Hunter: My name is Sarah Hunter. I am head of UK public policy for Google in the UK. I believe that we are here primarily to talk about our e-mail services. Just as background, Gmail—the e-mail service that Google Inc provides—has I think 425 million users worldwide. If you want to ask questions about any of our other services I will do my best to answer them but if there is anything I cannot answer I am happy to come back to you with written evidence, having asked my colleagues at Google Inc.

Stephen Collins: Good morning. My name is Stephen Collins. I am responsible for corporate affairs for Europe, the Middle East and Africa for Microsoft. I will not make an opening statement. You will have plenty of questions for us and we want to address what you are interested in rather than tell you what we think you should be interested in.
Emma Ascroft: My name is Emma Ascroft. I am director of public policy for Yahoo! UK and Ireland. I am here today representing Yahoo!’s UK business, but in order to be responsive to the Committee’s questions I will draw on the experience of Yahoo! Inc where that is relevant. I thank you for allowing us to do this session in private.

The Chairman: I understand that after we booked you for this session, the Home Office called you in for a friendly chat. Why, what was discussed and what was the tone of the conversation?

Stephen Collins: There was no formal consultation with Microsoft prior to this contact from the Home Office. It clearly contacted us having seen us being one of the companies giving evidence to the Committee. It was a video conference call with one of our lawyers. I was not in on the call. It was essentially to allow us to ask the Home Office questions about the draft Bill. I would say here that it struggled to answer most of those questions.

Q547 The Chairman: We will come back to ask you what it struggled to answer. Sarah.
Sarah Hunter: It offered us an opportunity to meet having seen that we were also a witness. We have not had a chance to set up that meeting, unfortunately. We have met it once since the Bill was published. Similar to Stephen’s experience, that was for us to ask it questions about the Bill rather than the other way around.

Q548 The Chairman: So in your case, it may just have been a coincidence that you were called in after we asked you to give evidence?
Sarah Hunter: It may well have been. I would not want to guess.
Emma Ascroft: This is going to sound like a familiar story. We were invited after the Home Office heard that we had been invited to give evidence to this Committee.

Q549 The Chairman: You had had no contact before?
Emma Ascroft: 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. I went on maternity leave at that time and made it clear that there was a colleague standing in for me who would be able to come to any meetings about this, but 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.

Q550 The Chairman: Let us go back to Stephen. You asked certain questions to which you felt that you did not get answers. What were those questions?
Stephen Collins: The ones where we did not get really specific answers, such as, “Can you articulate what the missing 25% of data is?” It could not really articulate what the 100% would look like, so it was difficult to see how it would get the 100%. On conflict of law issues, what if obligations that the Home Office placed on Microsoft put us in a position of legal conflict with home state laws? For us, that is those of the US, Ireland and Luxembourg. It could not really answer that. What if other Governments want access to the UK citizens’ data that we are
storing for longer now? That is a legitimate question that had not been put to them before, apparently. There is a whole series of questions.

Q551 The Chairman: You are reading from a brief there, Stephen. Would it be possible for the Committee, in confidence, to have that list or your brief?
Stephen Collins: [REDACTED]

Q552 The Chairman: We would be grateful. Okay, let us start with the 25%. Are colleagues content that we should pursue this line of questioning at the moment? Sorry, Sarah and Emma, did you have similar concerns about questions and answers?
Emma Ascroft: Yes, we had broadly similar discussions. There is a proposal in the Bill to require providers to generate data types specifically and only for law enforcement. That is over and above what a provider would generate and retain for their commercial purposes. We specifically asked what additional data types might be necessary, and the Home Office had to take that question away. From our perspective, the data types available to UK law enforcement, which it is empowered to request from Yahoo! UK, have not changed very much in the time that RIPA has been in place. We are not sure that there has been a loss of capability. That is why we asked what additional data types it might want us to generate. We are still waiting for a reply on that question.

Q553 The Chairman: By “additional data types”, what specifically do you mean? What would be examples of additional data types?
Emma Ascroft: The Bill is clear on what sort of broad categories of data it wants—traffic data, communications data and so on. Within that, there are specific data types, for example who an e-mail has been sent to and from. That is the kind of thing we mean when we say a “type”, and because we do not feel that the data types that law enforcement currently requests from us have changed significantly, we were trying to understand whether we would be asked to generate new types of data, as the Bill permits the Home Office to order us to do. It had to take that question away.
Sarah Hunter: I think our conversations were broadly along similar lines. The one thing I would add is that the intent behind the Bill of the officials we met seemed 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. We concluded that we would have to go away and understand more about the detail before we could give them a view on whether we thought it was reasonable or not.

Q554 The Chairman: So you are all worried that the oral assurances are reasonable and sensible. Everyone in this room wants to crack down on terrorists, paedophiles and drug dealers, but you are worried that the definitions in the Bill would allow a much wider data collection?
Sarah Hunter: I think that is a fairly good summary of our position.
Emma Ascroft: We are concerned on two fronts. There is what the Home Office says that it wishes to do, but we are not entirely sure that it is necessary and proportionate. The Bill itself is far broader and empowers the Home Office to do much more than what it has disclosed to this Committee. We have pointed that out to the Home Office, and pointed out the issue
around extending jurisdiction and the likelihood that this would set a global precedent. The UK would be the first country to extend its jurisdiction and take a reserve power to require UK providers to retain data that they could not obtain directly. We believe that other countries would follow, including countries that would use legislation of this kind to limit free expression and infringe privacy rights of internet users. From our perspective that would create a bewildering patchwork of overlapping and potentially conflicting legislation. Companies like us would face impossible decisions about how to be consistent in how we protect our users and operate our businesses in the 57 markets around the world where we operate. The Home Office fully accepts that that is a possibility; it anticipates that other countries will follow suit and seems quite comfortable about being the first country to do that. What is less clear to us is that it accepts responsibility for the consequences of that, which is a concern for us.

Q555 The Chairman: So if you let Britain do this and you are based in the States, you are worried that China or, hypothetically, Syria might follow. But then surely you would not give access to them. If it went to the FBI, through mutual legal assistance, to try to get it that way, America would say, “No, clear off China”. But you are worried that, although it may set a precedent, in reality it would be able to follow through and get the information.

Emma Ascroft: We are concerned that companies like us would be put in a position where we have to make difficult choices, when there are legal frameworks in place that specifically anticipate these issues around jurisdiction. Mutual legal assistance treaties, for example, specifically address the situation where data are required in evidence in one jurisdiction but fall under the jurisdiction of another country. They specifically acknowledge that that jurisdiction has limits, which is something that this Bill does not do. It does not place any limits on this extension to UK jurisdiction. That is where we have concerns. The Bill seems to be proposing an entirely alternative framework when there is one already in place and one which we would have thought was a more logical starting point for a policy review to address the concerns that the Home Office has presented.

Q556 The Chairman: So from Yahoo!’s point of view, if the Bill were to be enacted in its current form you would still prefer to go through with a mutual legal assistance route than comply with the Bill.

Emma Ascroft: 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. The concern with the Bill is that we are afraid that it will trigger and prompt other countries to make that legal environment even more complex when we are in a situation with overlapping and potentially conflicting laws that will put companies such as ours in a position where we have to make the decisions and arbitrate between the different legal systems. That is clearly what MLAT anticipates not happening; it aims to address that.
Q557 The Chairman: On this point of the route—whether to use mutual legal assistance treaties or implement the Bill—what is the opinion of Microsoft and Google?

Stephen Collins: The three companies are all set up legally and operationally in different ways. I can speak for Microsoft a little bit, having worked there previously. We address this matter in different ways. MLAT is not a big part of the process; we rely a lot on so-called voluntary compliance with RIPA as it stands at the moment, in accordance with US, Irish and Luxembourg law. The issue for us is that we have not been told by any of the agencies with which we work that there is a problem; we work very hard to co-operate with legitimate investigations that UK law enforcement and other agencies conduct. We understand that there is a need, but at the same time we try to balance a user’s right to privacy against those investigations. But it is an extremely co-operative professional relationship. It is perplexing to us, given the sudden appearance of this Bill with such broad ramifications, that no one will come and say to us that there is a problem, or that they do not have this or that data set, or that something needs to be for 120 days, not 90 days, and that that kind of thing is hampering their investigations. That is the perplexing part for us. One thing that struck me as I read the background brief from the Home Office to this draft Bill was that although it claims that there is an information gap I am not so sure that it is one—it is more a capability gap. There are multiple references to telephony in the background brief. My concern is rather that having got used to 20th-century technology and the data sets produced by it, using those very successfully in criminal investigations for evidential purposes—there has been a plethora of new data as mobile telephony has become a mass technology—they have become completely reliant on those data sets to pursue those investigations. However, on the 21st-century technologies, from companies such as ours and from others from which you will hear later today, we are not providing the same kind of services. A lot of the time they are not services at all; they could be semi-autonomous software applications. They generate different data sets. It is impossible to imagine attaching, for example, telephone numbers to a Facebook page or call data records to Skype video communications. It just does not work. So for me there is a danger that we are trying to address a capability gap when there is lack of capability of understanding among law enforcement agencies of 21st-century technologies and the data sets that are generated and how they can be accessed and used for investigations. It could well be that the data sets cannot be used in court as evidence currently, and maybe that is something that could be looked at. It could be that law enforcement needs greater training from industry and third-party specialists. I do not know what the solution is to bridge that capability gap, but it is like using a sledgehammer to crack a nut to try to introduce primary legislation on the basis of a supposed information gap that really does not exist.

Q558 The Chairman: I do not want to lose the point about the information gap, but I also do not want to lose the point about the mutual legal assistance treaties now that we are on it. What you have just said is crucial, and members of the Committee will want to explore it and whether there is a capability or information gap. Could I just finish off, along with any other colleagues who wish to ask questions, on the mutual legal assistance treaty, and Sarah’s view on it? If this Bill were to be enacted in its current form, how would you and your company feel about using that, or would you prefer still to use the mutual legal assistance treaty route for whatever reasons?
Sarah Hunter: At the moment, Google has a number of different ways to enable law enforcement to access user data. We have an emergency procedure, when there is an immediate risk to life, which is manned 24/7. Like Microsoft, we voluntarily comply with RIPA, to the extent that we can. For all other data requests we encourage Governments to use MLAT. We are supporters of the MLAT process. On Emma’s points about conflicts of jurisdiction, they do exist, and MLAT is designed to try to resolve those conflicts. We have heard informally that the MLAT process can be slow. My colleagues at Google Inc tell me that if that is the case, it is not the company side of the process that makes it slow; we therefore assume that it is the government side of the process that slows it down. I echo what others have said—that if there is a problem with that process it would be very sensible for us to start by looking at speeding it up and making it more efficient. The jurisdictional challenges that the Bill will provide will not make the MLAT less used; I think it might make it more used.

Q559 Dr Huppert: I was going to ask about communication with the Home Office, but I will stick to MLAT. What proportion of requests that you get from the UK do you currently comply with? Sarah Hunter: Google publishes a transparency report at www.google.com/transparencyreport. It breaks down how many user data requests Google Inc complies with across different countries. I think we complied with 68% in the last half year, so 32% we did not comply with.

Q560 Dr Huppert: How many of those involved MLAT requests?
Sarah Hunter: We do not break the figures down, but I suspect that that 32% would have been requests directly from the UK Government. We would then in some cases have pushed them to MLAT. I think that the US number of complied user data requests includes MLAT, and is a very high number; I think that we complied with something like 98% of US government requests, because MLAT comes through that. It makes our life a lot easier because Google Inc is a US company that is based in the US, and we have to comply with US law.

Q561 Dr Huppert: As I understand the Home Office’s intention with the Bill, it is that companies such as yours will be given a choice: “Either comply with what we would like you to do, or we will at least threaten to do DPI on transiting data and extract your data as they pass through the network”. Is that your understanding of the options, and how could MLAT fit into that as a third option? This Bill would empower the Home Secretary to say, “Look, you’re not prepared to have your data sucked in by the filter, so we will just collect it as it transits”.
Stephen Collins: On the particular point about DPI, I will not comment immediately. [REDACTED]

Q562 Baroness Cohen of Pimlico: The one thing that is obsessing the Committee is how much all this will cost. Therefore, when I listened to your description of the MLAT procedure, my first instinct is that it will be much cheaper to go via MLAT than to say to you guys, “Change your system so that we can suck off the data”. Is that perception faintly right? Let us suppose that you decided to co-operate with the Home Office rather than insisting it went through MLAT, and altered your systems so that you could do that. Will that cost a lot of
money? Under current legislation, the Home Office would of course remunerate you, but is it an expensive thing to do?

Emma Ascroft: Probably. As there is such a lack of detail in the Bill, it is difficult for us at this stage accurately to assess what the impact might be. That is one of the reasons why we are asking the Home Office for that detail. There is no doubt that if the Home Office asks us to generate data and retain them for longer, that will have an impact on our storage capacity and data-centre planning. The challenging part is not just the storage of the data but the retrieval. You can store much data, but you have to be able to search and retrieve them, and that computing power in technology that sits over the top of a data storage capability is the difficult and expensive part. We also expect that having more data would lead to more requests. That would have an impact on how we staff the team that responds to law enforcement requests. Therefore, speaking broadly, those are the categories of costs we would incur, but we cannot accurately assess the impacts until we have an idea of the requirements. However, as I say, the Home Office has not been able to tell us that; it will all come later in secondary legislation or in orders and notices. At the moment we do not have visibility of those, and neither would they be subject to further scrutiny. Therefore, this Committee cannot know what the full costs will be either, and we have to take it on trust.

Stephen Collins: On the MLAT point in Baroness Cohen’s question, the real issue is that MLAT is very slow. It is a government to government activity, so the costs to us would not be lower; we would merely receive the requests from a different court. That would be ideal for us, but we have to appreciate that law enforcement investigations sometimes have to move quickly, and MLAT processes can take months—multiple months—with some countries. We therefore need to keep in mind as well that if MLAT were to be investigated in order to be updated and improved with various individual second countries, it would require a big effort not just on the part of the UK but on the part of those other countries.

Sarah Hunter: I will just add an element to what Emma said. No one should be under any illusion about how complex, expensive and hard it is to secure user data at scale. Protecting a terabyte of data is very different from protecting a petabyte. As Emma said, it is not just about storing it but about being able to search through it and retrieve it. Our company runs search, and in engineering terms it genuinely is rocket science. So the more you protect, the more you require a communication service provider to store, the more you have to be able to search through it. That is very difficult. At Google, we employ, I think, 250 engineers just to protect data overlaps. This is not something that should be taken lightly.

Q563 Craig Whittaker: You mentioned in your transparency report comparable figures of usage for the UK, France and Germany. France is 44%, Germany is 45% and the UK is 65%. Why is there such a difference in giving information? Following on from that, Brazil has similar amounts and is at 90%.

Sarah Hunter: I agree they vary quite widely, and I am impressed that you know all the figures better than I do.

Craig Whittaker: It is called Google.

Sarah Hunter: Yes. I have asked my colleagues at Google Inc whether there is any more information that we can give, and the reasons vary quite widely. Sometimes it is simply that the form was filled in wrongly. Sometimes it is that the SPOC does not know what data are available. In those cases, the person at Google Inc who receives the RIPA request goes back to
the law enforcement agency and says, “Can you narrow it?”. Our Google Inc colleagues work with law enforcement agencies to ensure that they can comply wherever possible with them. I suspect that the reason why Brazil is slightly different might have something to do with the fact that we have different services there, in particularly Orkut, which is a social networking service that is very popular in Brazil. I can check and come back to you if you would like to know why Brazil is particularly different, but I think that it might do with that service.

Q564 The Chairman: Could we move on to the point that Stephen made about the 25% gap? He did not know where it came from. Can you explain your comments on capability versus information? You said in evidence that there is a huge plethora of new information, and you were not sure why the security service and the police needed more information and that they were not dissecting properly the information you were already supplying. Can you elaborate a little on that?

Stephen Collins: Of course. It is not necessarily that we are not supplying but that information is out there and could well be publicly available. I think that there is a lack of understanding not so much on the security service/related agency side but more on the regular police side. There is a lack of understanding of the potential for the pursuit of criminals from data that exist on the internet already. Let us take a concrete example. In the circuit-switch world, when people picked up a telephone a copper wire relayed the call to one other individual call data records were generated from one end to another end point and the telephone company knew both end points. That was the primary means of remote communication. Then we had mobile, which did pretty much the same thing but allowed you to walk around while you were doing it. However, it is not the same thing as communicating via Facebook. It is not the same thing as being in a multi-party video conference via Skype. These are different things; different data are generated. Different data may well be captured by Skype. They may be there but they might not be being asked for. I do not know unless we talk to the law enforcement agencies and the Home Office and they tell us what they think we are not currently supplying that they desperately need.

Q565 The Chairman: You have asked that question and they cannot elaborate on what it is they think they need or what they think is lacking?

Stephen Collins: They cannot elaborate on what the 25% is. Therefore, I cannot understand how they have worked out what the 100% is.

Q566 The Chairman: Emma and Sarah, do you have any comments or observations to make on that?

Sarah Hunter: We certainly did not have that figure of 25% shared with us. When we met the Home Office, it did not give us that number so we did not ask it about it.

Emma Ascroft: As I said earlier, we asked what the requirements of law enforcement are and, as the others have said, we have not necessarily had the operational feedback to say that we are missing stuff. That is why we asked the Home Office what additional data types it feels it is missing. The data types that are available to it now and that it has the powers to request are broadly the same as they were when RIPA first came into effect. We are therefore not sure that there is any loss of data with respect to Yahoo!. 
Q567 Craig Whittaker: We are also struggling to understand the 25% figure. In your expert opinions, as a percentage of the data out there, what could it use that it cannot currently get hold of?

Emma Ascroft: We do not know what the figure is, but from our conversation with the Home Office it seems that one of its issues is the availability of data. Its concern is around the MLAT process and its lack of timeliness. By the time a request reaches a non-UK provider, the data are simply not there. This is why we all share an interest. It is in everyone’s interest to see the MLAT process work more efficiently. It makes sense to make more use of MLAT not only from a legal point of view but from a practical point of view. If it could be made more timely, effective and efficient, it would be in everyone’s interest. Another tool that we think UK law enforcement could make use of is preservation orders for non-UK providers. In the US, for example, preservation orders are very widely used by US law enforcement. Where it has a particular target in mind, a US law enforcement agency can serve a preservation order on a communications provider and then preserve the data on a particular target so that they are not deleted in the time that it takes for the valid request to reach the provider. There are lots of ways in which UK law enforcement could work within existing structures to obtain data in a more timely way from non-UK providers. We just do not understand, because there has been no consultation, to what extent there has been a policy discussion in the Home Office exploring these very options. We just do not have visibility on that.

The Chairman: We had better get back on course.

Q568 Dr Huppert: I will look at the current law first, if I may. Is it clear what your legal obligations currently are, and would you welcome clarity in that? You talk about co-operating voluntarily, but does that expose you to legal risks if the US takes a different position?

Stephen Collins: [REDACTED]

Sarah Hunter: [REDACTED] We voluntarily comply with RIPA. My understanding from my colleagues at Google Inc is that that works fairly well. We have certainly had no complaints about the time it takes for us to respond to RIPA requests.

Emma Ascroft: [REDACTED]

Q569 Dr Huppert: Just to clarify something from slightly earlier, when Charles Farr gave public evidence to us for the first time, he said in response to Question 79: “Major CSPs understand the problem that we are trying to solve, understand the technology and the way in which we are proposing to solve it, agree that that technology is feasible and are looking for legislation to underpin collaboration in the future”. I presume you would consider yourselves as major CSPs? Would you agree?

Emma Ascroft: No. When the Home Office talks about major CSPs, it might be referring to traditional fixed and mobile operators. Certainly in our meeting, the Home Office spoke very confidently about its ability to order fixed and mobile operators to capture and retain data about third-party services provided by non-UK providers and about the willingness of those providers to do that. It also spoke very confidently about the capability of the technology—that the technology was there. We have had no contact with those fixed and mobile operators, so we cannot comment on their willingness to do that or on the technology, but that is what we heard.
Stephen Collins: The only reason why I imagine a company would welcome this Bill would be if it already provides outside RIPA and wants some kind of legal security to reduce its exposure. I do not agree with the evidence provided.

Dr Huppert: You think there are companies that do that currently?

Stephen Collins: No, that is just speculation. That is the only reason I can think of for any company welcoming the provisions of this draft Bill.

Sarah Hunter: From the Google perspective, Charles Farr’s characterisation of the conversation is not one that I recognise. Actually, in our meeting with the Home Office, we questioned some of the technical measures in the Bill, such as the request filter. I do not think that we agreed, shall I say, on its feasibility.

The Chairman: Could I go back to the international aspect and ask how your global organisations comply with the differing laws of different states? For example, what would you do if required by the UK to disclose data about a communication originating from, say, Germany, where the retention of data may be unlawful, or from Switzerland, which may have other secrecy laws? What would you do then?

Stephen Collins: If we received a valid RIPA request, we would expect the proper due diligence to have been done by the law enforcement agency concerned and the signing officer. If it was a court order issued by a judge, we would expect it to have determined that there was a sufficient nexus with the UK and we would comply with that request.

The Chairman: So if the SPOC has signed it off, even if it has come from Germany, Switzerland or Timbuktu you do not query where the originating e-mail or message came from?

Stephen Collins: Which SPOC?

The Chairman: You said that you would comply with it if it was a genuine RIPA request.

Stephen Collins: Yes.

The Chairman: However, the onus is therefore on the police officer or the security service to check that, wherever it has come from, it complies with UK law?

Stephen Collins: Correct, but it is not under UK law. If we are talking about RIPA and UK law, we will respond to a valid, properly authorised request. We will not analyse the content if it is properly authorised.

The Chairman: You will not look behind the communication to see whether it has come from, say, Germany or Switzerland?

Stephen Collins: As we action the request?

The Chairman: If the UK wanted you to disclose information on a e-mail or a communication that originated in Germany or Switzerland, where a different law may apply, you would not be concerned about that?

Stephen Collins: Again, the people who respond to the requests have a certain amount of expertise, but they are not international law experts. They would rely upon the assistant commissioner, chief inspector or whoever it was who signed off the request, and we would respond to that in good will, believing that the UK due process had taken place.
Q575 The Chairman: Is that the same for Google?
Sarah Hunter: I suspect that we might have a different approach. If we thought that there was a conflict of law, we would probably put it through MLAT. That is quite a good example of the challenges that operating our services throws at our colleagues who deal with them and why the MLAT process is so valuable. It is very hard to comment on a theoretical case without knowing a lot of the detail, but it is a good example because that is why MLAT exists.
Emma Ascroft: From our perspective, as I said earlier, we operate in a very complex global legal framework. There are many factors that determine which laws apply to a particular court request but, speaking generally, if a request came to us through RIPA and was served on our UK business and that data did not come under UK jurisdiction, we would ask the law enforcement agency to go through the MLAT process to the appropriate jurisdiction. [REDACTED] UK law enforcement knows well that if the data fall under US jurisdiction, they have to go through the MLAT process in order to obtain them.

Q576 The Chairman: What data would fall under US jurisdiction? Those of any customer on your server which is based in the States?
Emma Ascroft: As I said, many factors determine which jurisdiction applies. It is a bit difficult to talk hypothetically [REDACTED]
Sarah Hunter: It is worth pointing out though, from a Google Inc perspective, that we do not know the citizenship of our users. The only citizenship or geographical information we have is the location where they set up that e-mail address initially. Now, I may be on holiday in India when I set up a Gmail account in order to e-mail my family but I am a British citizen. These issues of citizenship are quite complex when you have a global service.

Q577 The Chairman: So what law might apply there? What jurisdiction would Google in those circumstances think was relevant?
Sarah Hunter: All of this is on a case-by-case basis; you have to look at the requests and the IP address. It is a complex judgment.

Q578 The Chairman: How relevant is the location of the server in deciding jurisdiction? Stephen, you say that you comply with British and Luxembourg—sorry, is it US and Luxembourg?
Stephen Collins: It is Irish and Luxembourg.

Q579 The Chairman: Is that because Ireland has the HQ and Luxembourg has the server?
Stephen Collins: No. Luxembourg has Skype headquartered there and Skype is now a subsidiary of Microsoft. The US has the headquarters, which is where the majority of data are stored, but for international services we also have a data centre in Ireland.

Q580 The Chairman: So what problems do you face in dealing with requests under RIPA because you have jurisdiction in Ireland and Luxembourg? Do you have to ensure that any RIPA request complies with Luxembourg and Irish law?
Stephen Collins: [REDACTED]
Q581 The Chairman: With Yahoo! and Google, is it similar or do you have servers in other countries as well?

Sarah Hunter: Our data centres are spread across the world. It is worth taking a step back to remind ourselves that Google Inc moves the data of its users between these data centres at a fairly rapid pace. You do not want to have one data centre holding all the data, because if it powers down overnight or it fails then it is very annoying to have lost all of your e-mail content. We spread the data across the data centres globally, so in those circumstances for Google Inc the US law is the primary decider for us.

Q582 The Chairman: Okay, so you all have servers spread across different countries. Taking up your earlier viewpoint, suppose that those countries say, “Britain is doing this; the UK is passing this new RIPA law. We want to do likewise”, then Luxembourg says, “Right, we want access to all of that as well”, and Ireland says the same—and with your server in India, the Indian Government hypothetically say the same. Do you see that as a risk and how would you handle that if it is a risk or possibility?

Emma Ascroft: Yes, it is a risk. This is a scenario that we discussed with the Home Office. We believe it is a very real scenario and, frankly, so does the Home Office. We believe that if the UK extends its jurisdiction in this way and takes the reserve power to require UK providers to capture and retain the data, if it is not available by extending jurisdiction, other countries will follow suit—and that will include countries that could use laws like this to limit free expression and infringe the privacy of internet users. As I said before, it 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.

Q583 The Chairman: Any other comments on that before we move on? No—you agree.

Q584 Lord Jones: I heard, and liked, your reference to the user’s right to privacy. That was in one of your earlier remarks. As a group of witnesses here, how often do you dig in over looking after the rights of the user? I heard the word “citizenship”, too, from one of you. How important is that to you and how far down does that commitment go in terms of your employees around the world?

Stephen Collins: From a Microsoft perspective—I am sure it is very similar for my colleagues—we would not have a successful business without the trust and confidence of our users. That is a kind of base assumption for building a successful business, particularly where there is an awful lot of competition in the marketplace and users can change to competing services at a couple of clicks of a button, so we have a robust privacy policy which we follow and implement rigorously. We have strict controls in place within our law enforcement response team—our global criminal compliance team, as it is known—in the US and, for Skype, a law enforcement relationship management team. They are trained to look at a request, check that it is properly authorised and undertake due diligence so that we can maintain this. It is a difficult balance, but we try to maintain the balance between co-operating with law enforcement and respecting the fundamental privacy rights of our users.
Q585 Lord Jones: Do you have many bust-ups? I mean: have you had distinguished cases on this?

Stephen Collins: With law enforcement?

Lord Jones: Yes.

Stephen Collins: [REDACTED]

The Chairman: Mr Wright, briefly, then we will move on.

Q586 David Wright: On the basis of that, what would be your market positioning reaction to this legislation in terms of the global market? Do you think that organisations such as yours, or even start-ups, will take specific decisions about UK law and about the way that they operate?

Sarah Hunter: Our position is probably very different to that of a British start-up which generally will not have a lawyer on its staff, for example, when starting up. We all have a number of lawyers. We are used to processing data requests and we are comfortable with that sort of relationship with law enforcement—and, as Lord Jones suggested, pushing back and being robust where necessary. For a British start-up, this Bill might put huge and unwieldy obligations upon them, such that it would put you off starting up a business. If you felt that you had to not only retain user data but potentially ask for extra data that you would not necessarily want to ask for, and then have it available to law enforcement, that is a significant cost. I think it would be very harmful to the competition within our sector.

Q587 David Wright: Miss Ascroft, you sort of said that your business was segmented in terms of its UK and US parts. Is there a threat that companies would start to say, “Well, we’ll close down the UK element of the business, focus all of our activity within US jurisdiction and segment our business structure differently”?

Emma Ascroft: Given our company structure, Yahoo!’s UK business would be subject to this law, however it would be passed by Parliament—

David Wright: Yes, that is what I am trying to say.

Emma Ascroft: So, yes, that part of our business would be captured. In terms of our other businesses around the world, it is the situation I described earlier in that we would expect other countries to follow suit and to pass very similar legislation. The Home Office anticipates that that is exactly what will happen and we will be in a very difficult position because our policy globally, as Stephen said, is that we are a company that is built on consumers’ trust and confidence, and in order to honour that commitment we aim to be consistent in how we engage law enforcement around the world. The consequences of this Bill would make it difficult for us to be consistent around the world, and we would then be put in a situation where we have to make very difficult decisions about how we engage law enforcement and how we protect our users. It is very hard to overstate the consequences of this Bill internationally for companies like ours. It really could be quite devastating on our businesses.

Q588 The Chairman: Google has pulled out of China, a mega market, because of various political reasons. Is there a possibility that if your American customers say, “Google, Yahoo!, Microsoft—you are co-operating with the British Government on this Bill so we’re not going to play with you any more. Close down your operations in Britain or we ain’t going to use
you, or we’ll use the Blencathra.com search engine instead, because you’re working with a Government who we don’t like”? How realistic is that threat, or is it fanciful?

Sarah Hunter: All our Gmail users are subject to US law, so our structures being different makes a difference in that respect. Our operations here are not the people providing Gmail services.

Stephen Collins: From the Microsoft perspective, we would not paint that sort of doomsday scenario. None of our services is provided from the UK currently. What large multinational corporations would look at, as they do already, are the compliance obligations for when they seek to invest in a country. It is a competitive environment; it is not just a question of whether or not you invest in the UK, but of where one invests. That is the crucial piece. To come back to start-ups, I share Sarah’s view. I do not want to exaggerate too much but there is a whole host of reasons, when one is involved in a start-up, for siting a company in a particular country. One of those that is taken very seriously is the regulatory burden. There are also the questions of access to venture capital, the amount of red tape and the qualifications of the staff but, when you are a two, three, five or 10-man band, this is an important consideration. You simply cannot tie up capital in unnecessary regulatory compliance when you can go to another market—although there are tax issues as well, of course—and not pay those regulatory compliance costs.

Emma Ascroft: Can I add another point? This might be a good time to talk a bit about our commitment to openness and user trust, and how that manifests itself in how the companies work together. We are all committed to protecting our users’ rights and privacy; together, Google, Microsoft and Yahoo! are founder members of the global network initiative, a global organisation that brings together internet companies, civil society groups, academics and investors specifically to develop a collaborative approach to protect and advance free expression. This organisation has developed principles and implementation guidelines that guide responsible company action in engaging law enforcement in response to valid requests for data disclosure. Those principles for all the companies concerned are a factor in guiding our investment and engagement in individual markets around the world. That affects not just markets around the world where there may be issues around human rights and free expression but also mature markets such as the UK. That is another factor that determines how we engage with law enforcement in different markets. You have heard separately from the GNI; it has given you written evidence, which will give you an idea of the kind of issues that companies like us face and how we work with human rights organisations to think very carefully about the impact of legislation and the way in which law enforcement operates on our commitments to user rights and openness.

The Chairman: We have covered a lot of ground. Baroness Cohen, could we jump to your Question 8, please?

Q589 Baroness Cohen of Pimlico: I think that Question 7 has been answered; we know that we are not very happy about being required to pass your data over.

If the legislation as envisaged went through so that a British-registered CSP was required to store your data in a way that it does not now, do you know what technical difficulties that would present for them?
**Sarah Hunter:** From Google’s perspective, all of the G mail traffic is encrypted by default and we are pretty confident about the quality of that encryption. It could be stored, but whether it could be read is another matter.

**Stephen Collins:** From the Microsoft perspective, all Skype traffic is encrypted, and increasingly encryption is being rolled out to enhance user privacy and security across the so-called Microsoft Live ID services, which include Hotmail. We would be in a similar position to Google, so presumably the data stream could be captured but there is nothing intelligible there.

**Emma Ascroft:** [REDACTED] We also raised questions about how the data would be secured and disclosed. We understand from the Home Office that, were an order to be served to a UK provider to capture and retain relating to a non-UK part of Yahoo!’s business, Yahoo! would not necessarily be told that in order had been served so we would not necessarily know that these data were being captured. We are also not entirely clear what the oversight mechanism would be within the oversight framework that is anticipated in the Bill—who would make sure that those third parties were capturing and retaining data in the right way, were not using them for other purposes, were storing them separately from their data and so on. That assumes that the data could even be extracted in the first place.

**Q590 The Chairman:** So you have said to the Home Office, “OK, you can tell Vodafone, BT and Everything Everywhere to capture these data but they are all encrypted, and neither they nor you can read them”—what did the Home Office say to that?

**Emma Ascroft:** We did not ask that question directly, but I believe that the Home Office has said to this Committee that it would not serve an order if the data could not be reliably extracted.

**Q591 The Chairman:** I just want to explore this point. You have told the Home Office, “Yes, you could store this material but it can’t be extracted”. What was the reason it gave for still wanting you to store it or getting others to store it?

**Stephen Collins:** But it was not for us to do the storage. The question is about the UK CSPs, the underlying network providers and access providers.

**Emma Ascroft:** The Home Office described this as a backstop power. I believe that it said to this Committee that it does not anticipate having to use it.

**Q592 Stephen Mosley:** [REDACTED]

**Emma Ascroft:** [REDACTED]

**Q593 Lord Strasburger:** What level of confidence do you have in your encryption, and how would you respond to a request either for the encryption key or for you to decrypt it on behalf of a public authority in this country?

**Stephen Collins:** For Microsoft it varies from service to service. I think that we will be talking about Skype in the next session, so I will elaborate on it there. Very briefly, there are no keys held by Skype to decrypt communications; they are discrete peer-to-peer communications where a private key pair is randomly generated by the software of the two end users. Skype take no part in that communication, so even if we wanted to we could not decrypt Skype-to-Skype communications. With SSL encryption, for example, I would have to get back to the
Committee on that regarding the precise methodology. I suspect that that would be possible but not easy. If you wish I will come back to you on the decryptability of SSL from originating providers, if that is helpful.

Q594 The Chairman: Have you had any discussions with the Home Office on potential legal liability costs that you might incur? This may be too hypothetical, but I can imagine that if we incorrectly ask for information from an American citizen, thinking that they are British or whatever, or someone with dual nationality, and that turned out to be wrong, we could have a multi-million pound lawsuit in the American courts and then joint action ones against you from another few hundred upset Americans, and massive legal costs. Have your lawyers have a look at this? Is there any concern that this may produce a new legal liability?

Stephen Collins: To be honest, this situation exists already, although maybe it would be exaggerated by the Bill. 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.

The Chairman: If they are going to collect a lot more information, there is a bigger risk.

Stephen Collins: That is quite likely.

Q595 Lord Strasburger: Lord Chairman, could I ask my encryption question of the other two panellists?

The Chairman: Of course. I am sorry.

Sarah Hunter: 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.

Emma Ascroft: I would say the same thing. If a valid RIPA request comes in, it comes with an obligation to provide the data in the clear. We would decrypt them. The encryption question is rather a red herring because the UK law enforcement agency can obtain the data direct from us using international legal channels such as the MLAT. If it came to us through those channels, we would disclose those data in the clear. If those channels work properly, this backstop power is unnecessary.

Q596 Lord Strasburger: You would provide that information decrypted?

Emma Ascroft: Yes, it is written into RIPA. Your obligation to disclose is to do so in the clear.

Q597 Craig Whittaker: I have two very quick questions. The first is on the encrypted stuff. Your data are captured by CSPs. How do you know whether that is context or content storing, which I believe is illegal anyway? Secondly—you may not be able to answer this question—how many countries subscribe to MLAT? Is there a possibility that, for example, Baghdad is not part of that process?

Stephen Collins: MLATs are bilateral agreements, generally. Not all countries are signatories with all other countries. I do not know what the list is for the UK; it is reasonably but not fully
comprehensive. There will be multiple countries that are not MLAT signatories with the UK. On the point about content versus communications data, it is a very hard thing to do. Even when one can see the content and the communications data, there are disagreements among experts as to what constitutes content and what constitutes communications data. The best example is website URLs—the addresses for websites—where it is quite clear that you can identify where a user is going. The usual example is AlcoholicsAnonymous.org.uk/help: if you go to that 40 times a day, that is a good indicator of your behaviour. It is not really about your traffic or communications data.

Q598 The Chairman: If you go on to it 40 times a day, there is not much time for drinking. I was not diminishing your point, and we have heard that point before. We are coming to the end of our session. Is there anything else that you want to impart to us? Are there any other areas, from what you have read about this, that you think we should be focusing on if we are to make sense of it?

Stephen Collins: Can I ask the Committee really to think about this notion of the past and trying to capture in aspic something that was beautiful 10 years ago—and trying to get back there. It is in the background brief. The Home Office states, “The Government is introducing legislation to ensure that communications data will continue to be available in the future as it has been in the past”. Another part says, “CEOP is already experiencing significant problems because of the difficulty of obtaining the same level of subscriber information for internet communications as is currently available for traditional telephony”. There is the problem. The key point is that our services cannot be made to look like telephony. We need better educated and trained police men and women.

Q599 The Chairman: Thank you. Anything to add to that, Emma?

Emma Ascroft: This is a global problem. The UK is not the only country looking at the challenges of a changing communications environment, the globalisation of communications and the changes in how users use those communications services. There were hearings on Capitol Hill last year where the FBI and Homeland Security said similar things. A consultation published in Australia in July is looking at exactly the same issues. It is a global problem that needs a global solution. The UK is the first country to have proposed draft legislation. It has done so relatively quickly without a great deal of consultation with the stakeholders who would be affected. Contrast that with the Australian process, where there is a consultation document out for public consultation now, a Cabinet committee has been convened to developed a terms of reference document that will also be subject to public consultation next year, and both Houses of Parliament are expected to do their own inquiries—and that is before draft legislation is published. The UK has gone out way ahead of the pack and the world is watching. If the UK passes this legislation, others will follow. We do not believe that that is the world that we want to create here. A more proportionate and less radical approach could be taken. We would welcome a sensible policy discussion on that. My second point would be that we must remember that MLATs are, by definition, a government to government process. The processes are defined by government and resourced by government. If they are not working effectively and efficiently and are not timely enough for the law enforcement agencies that they are intended to help, it is for the Governments involved to review those procedures and how they resource them to make them fit for purpose in this
internet age. We do not know whether that has been part of the Home Office’s discussions. That is something the Committee should invite the Home Office to comment on.

Q600 The Chairman: That is very helpful. We thank the three of you, and your supporting teams, for being frank with us today. We will have a complete transcript made and officials will discuss that with you. We are not going to suddenly publish that. If you—not just Stephen but the three of you—supply us with the questions you asked the Home Office and to which you would like answers, maybe we can also ask the Home Office those same questions. We have an idea what some of them might be, particularly on cost and so on, but we would love to know the questions that you want answered. We will have a go. Thank you very much for coming today and good luck in future.

Sarah Hunter: Thank you.

Emma Ascroft: Thank you very much.
Evidence heard in Private

**Facebook [Simon Milner], Twitter [Colin Crowell], Skype/Microsoft [Stephen Collins], and Tor Project [Steven Murdoch] (QQ 601-659)**

**Examination of Witnesses**

**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

Q601  **The Chairman:** Welcome everyone. We are in private session with our visitors and we will now start record recording. A warm welcome to you and thank you very much for coming. This is a private session and the people in the room are the Members of the Committee, our officials, clerks and our Lords and Commons transcribers—and no one else. Perhaps I may identify people and make sure that no one has crept in you. Will those supporting Mr Murdoch put your hands up?

**Steven Murdoch:** There is no one with me.

**The Chairman:** Is anyone supporting Simon Milner? Simon, could you turn around and confirm that those two people are with you?

**Simon Milner:** Those people are with me, yes.

Q602  **The Chairman:** Stephen, your people again? And Colin Crowell? Good, that is excellent. We are all complete. Thank you very much for coming. Thank you to those who have given us written evidence. This is a private session. We will be making a transcript but we will not automatically publish it. We would like to show it to you and discuss it with you. If our clerks and you can discover anything that we feel is safe to put into the public domain, by agreement we would do so. But we do play fair—if we tell you it is private, it is private. I hope that will encourage you to speak frankly to us. We all want to have powers to deal with terrorism, paedophiles and drug dealers, and we as parliamentarians have to balance that against the privacy of the individual. If we are to get this Bill right, we need to get from you a frank analysis of its strengths and weaknesses. We prefer to get that in private, even if we cannot talk about it afterwards, than for you to sit there and not spill the beans on what you think is right and wrong. If you do spill the beans on things that you do not want public, we will not make it public, but ideally we want to hear it. For the record, could you briefly identify who you are?

**Steven Murdoch:** My name is Steven Murdoch. I am with the Tor Project and I am also a researcher at the University of Cambridge.

**Simon Milner:** I am Simon Milner. I am director of public policy for Facebook in the UK and Ireland.

**Stephen Collins:** Hello Committee, I am Stephen Collins and here again. This time, I am wearing the hat of Skype. Until six months ago, I was head of regulatory affairs and global law enforcement relationship management at Skype.

**Colin Crowell:** My name is Colin Crowell (@Colin_Crowell on Twitter). I am head of public policy for Twitter.
Q603 The Chairman: Excellent. Thank you. Perhaps we can begin. I understand that some or all of you, after we asked you to give evidence, may have been asked to go to the Home Office for a discussion. Is that right? What was the discussion about?

Simon Milner: On behalf of Facebook, I am happy to confirm that, yes, we were invited to a discussion at the Home Office. It was our second meeting with the department since the Bill was published. We asked questions about the Bill and provided some other perspectives that I going to share with you as part of this session today, in particular our concerns around some of the provisions in the Bill.

Q604 The Chairman: But you had dialogue with the Home Office before we asked you to give evidence to us?

Simon Milner: Yes, but only after the Bill was published. We had no dialogue with the Home Office before the Bill was published.

Q605 The Chairman: And you had no input? You did not write to them and give it?

Simon Milner: We were never asked and we never provided it.

Steven Murdoch: The Tor Project has not had any communications with the Home Office about this. We have not been invited and we have not had talks with them.

Q606 The Chairman: Briefly, Stephen, you are at the same point as before.

Stephen Collins: Yes, exactly the same, so I shall not waste time by repeating it.

Q607 The Chairman: And Colin?

Colin Crowell: We had one conversation with the Home Office about two and a half weeks ago. So we, too, were contacted after the Bill had been published and had one phone conversation with them about it.

Q608 The Chairman: That contact would be after we asked you to come here and give evidence.

Colin Crowell: Correct.

Q609 The Chairman: I see. So some of you had discussions with the Home Office via either teleconference or face to face. What was it about? Were you raising questions?

Simon Milner: Yes. In our case, we were asking questions in particular about the data retention proposals and what the Home Office had in mind on what that might mean for Facebook. It explained that to us that the Home Office envisaged that there would be a retention order on Facebook to retain all communications data in respect of Facebook users in the UK for a year. That gave us grave cause for concern about such a blanket retention requirement being placed on us. We also talked about the access process, but we were particularly focused on the retention regime in that conversation.

Q610 The Chairman: And Mr Crowell?

Colin Crowell: Yes, our conversation with the Home Office was similar in that it largely focused on asking questions about the intent of aspects of the legislation as we read it. The
legislation is largely enabling, with lots of the implementing regulations and orders to come. Subsequently, sir, we were curious as to how they saw it working in practice. We also had questions about the assertion of authority to a company such as Twitter, which is subject to US laws, and the relationship that we might have with a communications carrier here in the UK and the acquisition of our users’ data and the retention of that data here.

Q611 The Chairman: Mr Milner and Mr Crowell, you were concerned about retention for UK users. Where would those data be retained? Would it be in the US or in servers in UK?
Simon Milner: As regards the UK, it might be worth the Committee understanding our user base here. We have around 30 million active users in the UK and around half of them will log on to Facebook every single day. All our data are held in data centres in the US, and therefore I envisage that we were subject to an order that these data would be retained in a data centre in the US. That is what the Home Office envisages as well.

Q612 The Chairman: Do you have concerns about that or are you relaxed about it, irrespective of the cost?
Simon Milner: We are very concerned about it.

Q613 The Chairman: What would the concerns be?
Simon Milner: In respect of the cost benefit of such a measure, we would be asked to retain enormous amounts of data which we would ordinarily delete if the customers asked us to do so. For 30 million users, only a tiny fraction might be subject to a request as part of a law enforcement investigation, but the data set would be there and it would be known that it existed. Law enforcement agencies in other countries might also seek access to those data via the US courts. We think that that should be a real concern for the UK citizens and for Members of this Committee.

Q614 The Chairman: Mr Crowell, is that a similar concern?
Colin Crowell: Yes, it is similar. Our servers are also in the United States, and one of our concerns would be about a UK-based carrier ordered to collect Twitter data here in the sense that our user data would be retained by a UK carrier. That would therefore pose problems to us in terms of our terms of service and privacy policies. If such an order were to come to a domestic carrier here, that would collect and warehouse our data. We would also have issues with respect to not knowing when an access request for such user information was served on the company that was UK based and collecting our data. Finally, it is not clear how the filtering regime that is outlined in the Bill would work in practice, even from a technological standpoint.

Q615 The Chairman: We will come to the technology in a moment, but let us just park it if we may. If I am tweeting a person in the States and you are asked by the British Government to store those data, presumably data on the person I am tweeting in the States would have to be stored as well, or at least part of it.

Q616 Colin Crowell: Yes, if it is a direct communication back and forth between two users, we would store both.
Q617 The Chairman: The same would apply to Facebook, I presume

Colin Crowell: It is a real conundrum from a jurisdictional standpoint how we would deal with user data that might be related to non-UK citizens that might be part of a communication with a UK citizen. There is also the issue that it is not just as simple as solely dealing with the United States; often people are communicating with other people in various countries around the world.

Simon Milner: Further to Mr Crowell’s point, we would strongly oppose any measure that required us to violate the law in another country. One thing that we would expect to result from a discussion around an order would be that we would want the UK Government to frame an order so that we were required to retain data only in respect of UK users, otherwise we might be violating the law in the US or, more likely, other European countries, given the data protection framework. So we would store data only in respect of UK users. If the Government sought to propose an order requiring us to maintain data about users in other countries, we may well have to seek a solution which involved the courts. We would not want to do that; we think that that kind of conflict over jurisdiction does not help the primary purpose of this measure, and in terms of our good relationships with law enforcement we would not want to have that kind of conflict over jurisdiction. But it seems inevitable that that is likely to result from this measure.

Q618 The Chairman: So if I or any other British citizen sent a message to friends in Switzerland or the United States and it is contrary to Swiss or United States law to store it, you would have to develop a system whereby you stored only my half of the message?

Simon Milner: That is what we would envisage would be the only way to ensure that you could be able to comply with UK law, as we would of course want to do, and comply with the law in other countries. To give an example of what kind of data that might result, you might have a record that says that UK user A communicated with UK user B, and then with somebody else somewhere in a foreign country, but with no information about where that person was or what country they were in—only that there was a communication with somebody else via Facebook. We struggle to see how that will be useful for law enforcement.

Q619 The Chairman: I can immediately see the gaps, but if that is your view of what you would have to do legally it is worthwhile information to have. My final point on the international aspect is this. If 30 million British subjects are held on a server in the States, do I understand the Patriot Act and others correctly in thinking that American authorities, whether the NSA or the FBI, would then have the right to say that they wanted access to anything on an American computer?

Simon Milner: Well, we are subject to the US courts, and if we receive a valid and enforceable order requiring us to disclose data about a user we have to comply with that order. It is worth bearing in mind that UK users of Facebook have a contract with Facebook Ireland and are protected under Irish data protection law, which is under the European data protection framework. We are subject to some very clear and robust rules around how we handle their data. It is not an issue that has arisen thus far, but you are right that, given where we hold our data, it could be an issue in future.
Q620 The Chairman: Is it fanciful that American security agencies could serve a legal notice on you, saying that they did not just want information on this dodgy character, Blencathra, but on all 30 million Brits so that we can do a trawl for other reasons.

Simon Milner: The approach of the US authorities has been much more around preservation than retention. You might get requests to preserve data about accounts of somebody of interest, who may well be suspected of illegal behaviour. So it would be completely out of character, given their approach to these issues, to take that kind of blanket action.

Q621 The Chairman: And Twitter is of the same view, roughly?

Colin Crowell: Yes.

Q622 The Chairman: Can we move on to the third question?

Q623 Dr Huppert: Mr Murdoch has been a bit silent so far. Tor has a slightly different relationship to this. What would be the consequences of this Bill on your operations? Are there specific consequences that you would have directly?

Steven Murdoch: In some sense that is difficult to say, because the Bill does not go into very much detail. The Tor Project or architecture is very different from these other systems. We do not process the communications of the users. People who use the Tor network download the software from us, but their communications go over servers that are operated by volunteers to which we do not have access. Because we have designed the system to have privacy from the start, we would not technically be able to hand over any communications data, regardless of whether we were ordered to do so. Whether we fall under the legislation at all is an open question, and we have not had any guidance as to what they believe. If we did, we would have to substantially change the architecture of Tor, and basically rewrite it from scratch, before we could do anything useful to provide communications data. Long before that happened, our funders would pull out and the users would pull out and the project would effectively cease.

Q624 Dr Huppert: It is helpful to understand that. There is an issue about the gap that the Home Office says that it wants to close. How often do you get data requests at the moment that you are unable to satisfy or that take a very long time to satisfy? Do you have experience of the gap existing when you get requests that you cannot satisfy.

Stephen Collins: Maybe I can kick off for Skype. I have been very quiet because I did not want to repeat everything I said in the last session. In the early days of Skype, we had all sorts of fanciful requests; it took a lot of time and effort on our part to educate particularly the SPOCs, specifically in the UK. We have built up a very good relationship with various constabularies around the UK to make them understand what Skype is and what it is not—a telephony service. It is a peer-to-peer software. We tell them how it works and what data we can usefully provide to them on receipt if a valid request. These days we get very few requests that are technically inept, if that is what you are pushing at. There is a good understanding not so much among the regular police officers but among the SPOCs at least, and we have spent a lot of time and energy to try to educate them so that they do not waste their time, and ours.
Q625 Dr Huppert: It is not just technically inept requests that we are talking about. There are also cases where there is a technically ept request, if that is a term, which asks for data that you do not have, but which under this Bill you would have.

Stephen Collins: Still for Skype? The data that are generated we will make available, if it is in a useful and accessible form. We have made it quite clear what those data sets are to the law enforcement community in the UK.

Q626 Dr Huppert: So the Bill would not have an effect on the data that be obtained from Skype?
Stephen Collins: The Bill would not apply to Skype.

Colin Crowell: We probably get fewer requests for user data than some of the other services, only because the nature of Twitter is that most of what happens there is already public anyway. Law enforcement oftentimes simply has to go to the web on its own and can obtain the relevant Tweets that they were looking for. We probably get fewer requests there. With respect to the gap and a request for greater data collection and retention, Twitter also tends to collect less user data than perhaps some of the other services. For example, we do not collect information from our users about gender, age, home street address or things of that nature. If there are personal data that we have no legitimate business reason to collect, we do not gratuitously collect it. The irony, in looking at this Bill, is that on most of the other panels that I tend to appear, the policy makers and elected officials are urging us to collect less data and engage in data minimisation, rather than to collect more. The provisions of the Bill that hold out the possibility that we may be compelled to collect data that we have no legitimate business reason to collect is also a concern for us. We would have to explain to our users why we were collecting it and for whom.

Steven Murdoch: Like Twitter, the data that we can disclose to law enforcement are public anyway, so most of our effort goes into training law enforcement as to what Tor is, what data are available and how it can make use of them.

Q627 Dr Huppert: So you do provide some data?

Steven Murdoch: The data that we provide are to confirm or deny that a particular request came through Tor. So we can say that a particular IP address was a Tor server at a particular point, and that can guide future investigation. We provide that information, and we also provide software to law enforcement or to anyone else that will allow them to find that information without contacting us.

Simon Milner: We have a dedicated team in our headquarters in California and in Facebook Ireland that handles requests from law enforcement. The team in Dublin handles requests from the UK authorities for standard requests. In emergencies, our Californian team can also help with those requests. Based on the feedback that we have from UK law enforcement [REDACTED] they have indicated to us that they are very happy with the relationship and the turnaround times within which we provide data. I believe that they would be in a better position to identify specific cases, if any, in which they ask for communications data that we are unable to provide, either through that request process or through the MLAT process.

Dr Huppert: No one seems to be able to put their finger on it applying to them, which is one of the problems that we are having.
Q628 Baroness Cohen of Pimlico: The actual legislation on data might require a British-based CSP to store the data as opposed to you guys. The onus in default is on that CSP. I think you have answered the question whether it will indeed alter your relationships with everyone who finds themselves having to do this. If a third-party CSP was told that it had to pick up your data as they went across it, is this technically very easy for it? What difference does encryption make?

Simon Milner: I am happy to start on that. I think it is for them to advise you on the technical difficulties of collecting third-party data.

Baroness Cohen of Pimlico: Indeed.

Simon Milner: From our perspective, rather as Mr Crowell was saying, we are often asked to testify about data minimisation. As you can imagine, 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.

Steven Murdoch: We are also very concerned about the possibility of third parties intercepting data going to the Tor network. The design of Tor mitigates the potential harm from unauthorised interception or the abuse of intercepted information, but it does not eliminate it. We are also very concerned about other systems going over the internet which human rights workers make use of but that do not contain the protections that Tor has. Going back to Tor, it would be possible to intercept the data, but there are some technical challenges. One of our design requirements is that it should be hard to distinguish Tor traffic from other internet traffic. We need this to resist censorship in places such as Iran, Syria and China, so our traffic can look like web browsing or Skype. It can look like many different things, so it would be hard to pinpoint it.

Stephen Collins: [REDACTED]

Q629 The Chairman: [REDACTED]

Stephen Collins: [REDACTED]

Colin Crowell: It is fair to say that no company would want its user data collected and held by another company. We have to hold ourselves out to our users and to US regulators and assert that we take steps to secure our user data and protect it from compromise. This might be a situation in which our user data are held by another company and we have no control over the security features that it brings to bear in storing that data. Secondly, there are the competitive issues and concerns that Mr Collins just raised. The technical aspects of achieving it are tricky, and one of the things that have been a characteristic of the internet marketplace, especially for a lot of the services that are web-based, such as the over-the-top services, is that they are in continual evolution. The features and services that we roll out will change from time to time from a technological standpoint, and there has often been this technological one-upmanship, with varying degrees of encryption and countermeasures for that, and so on and so forth. This would not be a static technology that is deployed once and then is there for use. It would
involve measures on the outside coming in, and it would have to reflect how it could implement the filtering regime, as outlined in the Bill, to adequately tease out just the information that constitutes the communications data that might be relevant for an investigation as opposed to the other content and data that might be part and parcel of those packets. The final point I would make is that, to the extent that this is implemented in the UK, other countries might seek to do the same. So the paradox may be how British internet companies and British citizens might feel if a similar regime were instituted abroad.

Q630 Baroness Cohen of Pimlico: We are wondering what the implications would be of requiring a British-based CSP to store some of your data that go across it. Are you suggesting that your reaction would at the very least be to encrypt to protect your customers?

Colin Crowell: I do not know how we would ultimately decide to deal with a situation like that. We may have duties in other jurisdictions to protect data that may reflect on how we provide our service. The other aspect, which Mr Milner alluded to, is that our users also have the ability to encrypt. So even if Twitter were not to do so, a user could encrypt on their own.

Q631 The Chairman: We assume that the order is given to the Vodafone, the BTs and the Everything Everywhere of this world to say that the data of yours that they intercept or that pass through their network have to be stored in the UK. Would you have a view on that? Would you want to see that in the Bill, or would you have concerns about how data from your network might be stored by a United Kingdom telecoms provider, shall we say, on their farm in India or outside the UK?

Simon Milner: From our point of view, that is a far lesser consideration than the fundamental issue of their being asked to store it at all. The location where they store it is less important than that.

Q632 The Chairman: So storing it in London is just as bad as storing it in Mumbai?

Simon Milner: Absolutely.

Stephen Collins: Before we consider that question, another question to ask is: 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?

Q633 The Chairman: [REDACTED]

Stephen Collins: [REDACTED]

The Chairman: I read a brief yesterday suggesting that DPI technology lagged a few months or years behind the innovations in technology for providing new services.

Stephen Collins: It is an arms race.

Q634 The Chairman: Is that correct, and what are the problems that it encompasses?

Stephen Collins: Is that from a Skype perspective?

The Chairman: Or just from an industry perspective.

Stephen Collins: I do not want to speak on behalf of my colleagues, who may take a different view. From our perspective, 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.

Q635 The Chairman: But if people are to comply with the Bill, you as service providers cannot introduce a new service and then wait a few months or a couple of years for the DPI technology to catch up. Would you be under an obligation not to launch your new service until there was the DPI to analyse, record, check or store it?

Simon Milner: If I might say so, one of the issues that this raises is how these orders are going to be determined. From our conversation with the Home Office, the clear sense was that it expected them to be negotiated; the Home Office would not simply write them and turn up on day one after Royal Assent with the order written. To some extent, there is a degree of comfort in that in that it recognises that it is going to have to take account of some very different services and situations. The Home Office also indicated that it saw imposing these requirements on the CSPs very much as a last resort. To our mind, that again is recognition that the Home Office has not really thought this through very well if it is a key part of the legislation but it is telling us about it only after the Bill has been published. It makes us feel rather worried that there is a sense of, “Don’t worry, we’ll sort this all out in the end once the Bill is passed”. By then, though, parliamentary scrutiny is finished, and from our perspective that is not a good place to be. We would much rather be having those conversations well before any draft legislation is published.

Q636 Lord Strasburger: I am still in search of this elusive 25%. If representatives from the Home Office were here today—and we asked them—they might say that telephony was not all on landlines or even on mobile phones but is now over the internet, and they might point at Skype or Tor as developments that have reduced their capability to capture and retain information. Would it be true to say that, in the case of Skype and Tor, even after the Bill is passed the Home Office will be no further forward, because you do not hold in your organisations the information that it would need to make any sense of those communications? In the case of Skype, it is peer-to-peer encryption and you do not hold the keys, so you cannot help the Home Office. Am I right in saying that?

Stephen Collins: That is correct. That is a content issue, but Skype does not operate like a telephony service. Those data are not generated, and we would have to make incredible architectural changes—rewrite code—in order artificially to generate some kind of telephony-like data.

Q637 The Chairman: If you were ordered to do it?

Stephen Collins: I guess there would be a question whether a Luxembourg software provider could be ordered or compelled under the terms of a UK Act that applied to communications service providers, which Skype clearly is not when you read the definitions. So there is both a definitional piece and a jurisdictional piece that I would say exclude Skype from the RIPA terms.
Steven Murdoch: Tor is a US-based organisation, so if the Bill could be applied to the Tor Project—because the reason for the Tor Project existing is to protect the safety of users—we would be in an even more difficult position than Skype in implementation. We would almost certainly fight this in the US courts, and if it came to the point where we could not operate in the UK, we would sooner not operate in the UK rather than basically destroy the project.

Q638 Lord Strasburger: I understood you earlier to say that you do not possess the information that would enable the police or the security services to unscramble what has passed through your servers. You just do not possess it.

Steven Murdoch: Yes.

Lord Strasburger: So whatever legal obligations are placed on you, you just cannot give it.

Steven Murdoch: Yes, and under the current design we do not have access to those data. We would have to build something different from the beginning before we could be in a position to collect any of them.

Q639 The Chairman: Did the US State Department encourage Tor to be set up, or does it back it?

Steven Murdoch: The Tor Project was originally found by the US Navy Research Laboratory. Most of its funding now comes from Governments and most of that comes, one way or another, from the US Government.

Q640 The Chairman: So the United States Government might have a view if the British Government wanted Tor to spill the beans?

Steven Murdoch: Yes. From speaking to the funders, it seems that they do not want anyone, including themselves, to have access to communications data because they are so sensitive for the safety of the users and there is no safe way to store them.

Q641 Lord Strasburger: Lord Chairman, I understood the witness to say that TorR does not possess the keys or the ability to unlock this information. It would have to completely change its architecture. Is that right?

Steven Murdoch: That is correct.

Q642 Craig Whittaker: Most of my questions have been answered, but can I come back to you, Stephen? You said a couple of times that Skype would not come under this legislation. If the traffic was going across UK communications service providers, surely it would—and whether or not that is captured by you or by those CSPs, you are going to get caught up in this anyway.

Stephen Collins: We will not be caught up; if that were the route that the Government decided to take, it would be the CSPs. Skype would have no involvement. There is nothing that Skype could do about that from a legal perspective, but it would be for the CSPs, with their DPI equipment, to seek to capture those encrypted data.

Q643 Craig Whittaker: [REDACTED]

Stephen Collins: [REDACTED]
Q644 Craig Whittaker: [REDACTED]
Stephen Collins: [REDACTED]

Q645 Craig Whittaker: [REDACTED]
Stephen Collins: [REDACTED]

Q646 Lord Strasburger: And what information are you able to provide?
Stephen Collins: [REDACTED] It is essentially subscriber information at the time of registration, which includes a variety of non-verifiable information: an e-mail address and an IP address at the time of registration. Then we have some communications data and call data records for some of the ancillary services such as SkypeOut, which allows you to call from Skype to a regular telephony service. Those CDRs, as they are known, are available, and there are one or two other things such as that concerning instant messaging.

Q647 Lord Strasburger: But Skype to Skype is entirely subscriber data?
Stephen Collins: Yes, because there is no service involved there. It is a self-provided service, and if you and I are communicating on Skype, our Skype clients and our computers are talking directly; they are not routing through Skype. All Skype has enabled us to do is to get into the peer-to-peer network. Once we are in, there is a distributed directory, which we do not control, inside the network on so-called super nodes. I do not want to get too deeply into this, but we can find each other without Skype’s help and then our software sets up a call between us. Skype has no involvement. That is where the private key exchange of encryption keys takes place. They are randomly generated by the software and then discarded when the session that we have ends, so if we spoke the next day it would be a different encryption key, randomly generated by those two. Skype cannot see that and has no involvement in that process.

Q648 Craig Whittaker: I have a final question, as I want to go back to this 25% figure that the Government have said is a gap. Is that a genuine “We don’t know what 25% is”, or is that just because the law enforcements do not ask any additional questions of you, because they already know what they can legally ask anyway? Does that make sense? Can you envisage what a proportion of the 25% is at all, or is it just because we ask you only what we ask because that is all we can legally ask you?
Stephen Collins: It could be, for example in the case of Skype, that they do not get full call data records for Skype to Skype communications. That may be it—I do not know—but how can that be missing when it never existed? It does not exist. It is not a telephony service.

Q649 Baroness Cohen of Pimlico: It seems to me that, at least on behalf of all the over-the-top services, the power for UK CSPs to collect your stuff as it goes over them is actually not useful. Would that be fair? So one then asks oneself, "Why is it in the Bill?". Is there any evidence you can see to suggest that it is a negotiating position for the Home Office to say to you, “Look, we’ll claw it off by DPI”, even if you really know that they cannot? I am asking you only to speculate about why the Home Office should want this power, because it is not obvious from the answers to your questions.
Simon Milner: I think you have had the Home Office here to provide evidence on understanding quite what the thinking is behind that. As you say, it may be part of their negotiating armoury when it comes to discussing an order with a company such as ourselves, or others at this table.

Baroness Cohen of Pimlico: It is, in short, ad terrorem.

Simon Milner: Your Latin is better than mine.

Q650 Lord Strasburger: I know that we are stuck on this one issue but it is very important. Can I ask the question the other way around? If this Bill were enacted, how would the access to data of the public authorities that request data be improved, as far as you can see, if at all?

Stephen Collins: From a Skype perspective, I do not think it would be improved.

Simon Milner: From a Facebook perspective, in situations where a user has asked us to delete data and we are under an obligation to delete their data, if we are now required to retain their data, then in theory, of course, in respect of the odd individual user some data might be available that is not currently available. However, that would come at a very expensive cost in terms of the engineering effort that would be required by us to retain data that we currently delete—and which all our systems are set up to delete—for tens of millions of users, possibly just for the odd one or two requests that cannot currently be fulfilled to be fulfilled. Hence the sense that this is absolutely a sledgehammer to crack a nut. Yet the nut may not even exist, and we are not really sure how small it is if it does.

Colin Crowell: As I mentioned before, most of what occurs on Twitter is already public anyway and, typically, law enforcement simply has to go to the web and search for it. Where they are looking for particular non-public information or subscriber data, we do not get many of those requests, but it is Twitter’s policy to preserve evidence as soon as we are informed formally by British law enforcement. If they have a particular suspect or account that they would like the non-public information from to build a case here in a non-emergency context, we preserve that evidence while the legal process runs its course to convey it. Part of this is also taking two steps back and going back to the question of what the problem is that is being posed here. What is the problem that we are trying to solve? Going back to the question about the 25% gap, it does not seem to apply to Twitter because of course there is more information about what people are tweeting that never existed in the telephony world before, so there is more information there. Voluminous amounts of data on users from myriad companies could be collected through deep packet inspection technology. Again, that is what is being proposed to gain access to the few accounts where they may subsequently seek to build a criminal case.

Steven Murdoch: In the case of Tor, it would not make a significant difference. In the case of some other internet services, it could give access for the law enforcement agencies to more useful information. But criminals already have the capability to prevent law enforcement making useful use of communications data. Criminals have shown the capability, but human rights workers do not have the same capabilities that criminals have, so they will be put at risk by deep packet inspection and similar things that this Bill could introduce.

Simon Milner: Could I suggest that this could make this worse?

Q651 Lord Strasburger: Can we just stop? Sorry, but the Bill does not introduce deep packet inspection. The Bill introduces the wholesale retention of everyone’s data for a period of 12 months. Deep packet inspection is a red herring as far as that is concerned. My question is:
what does the wholesale retention of communications data over a period of 12 months do to enhance law enforcement and all the other agencies who want to get this? The message I am getting from the whole panel is that apart from, perhaps, some Facebook accounts that might have been deleted over that 12 months, there is nothing.

**Simon Milner:** In fact, it could make things worse by redirecting resources in an inefficient way. In the context of how we currently work with law enforcement, you have heard from all of us that we already have some very effective arrangements for dealing with law enforcement and for providing information to lawful requests on a timely basis. Those are improving all the time and we have dedicated resources for doing so. Were this Bill to come in, one would expect that there could be quite an extended period in which some of those resources are being used to negotiate over a very difficult kind of order, with lots of resources focused on how much this is going to cost and on the engineering involved in it. [REDACTED]

**Q652 The Chairman:** Lord Faulks will want to come in on costs in a moment. First, just to finalise that point, how worried are you that if relations get soured, it will go back to the lawyers who will say, “Okay, give the Brits just what the American law requires and that is it”? Is that a real risk?

**Simon Milner:** I hesitate to say what would definitely happen. We are at an interesting stage in this process. It will be interesting to see how the Government react to this Committee’s recommendations. We very much hope that will not happen, but it is certainly a scenario that one could imagine playing out if the Bill were to stay as it is and if the Home Office’s approach to it is as blanket as it has suggested to us.

**Q653 Lord Faulks:** You have answered quite a lot of the points that I wanted to raise anyway. Very briefly, I detect that one of the real problems for all your organisations is the uncertainty and quite what it will mean in commercial and cost terms if the Bill becomes law. Have you made some estimate in your own minds as to what the costs will be? Bearing in mind that you can of course recoup those sums from the Government, have you any general comments beyond those that you have already made in that respect?

**Stephen Collins:** 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. That is very difficult. We know how much it costs to retain data. We could calculate on that basis. What would not be in the cost-reimbursable piece are all sorts of other things that have not been considered by the Home Office. Those would include things such as additional hardware databases for segmentation of the data from UK users—even if we could identity them, which I am not sure we could—into separate databases. A part of 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. We will need redundant systems, so everything would have to be duplicated and put into two locations. We have ongoing personnel costs to manage all these new sites and databases and to respond to requests. There is a whole host of other costs that are not considered at this stage by the Home Office. It appears that it has just looked at the cost of data storage. That is just the tip of the iceberg in cost terms.

**Q654 Lord Faulks:** So you do not think that its estimates are realistic?
Stephen Collins: I think they are really unrealistic—and 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.

Simon Milner: I very much support what Mr Collins said. In the same way as we do not understand how the Government have worked out their numbers, I cannot give you a number because we simply find it very difficult to understand what is actually being required of us. We expect that this would be a very significant engineering project. The comparison I would make is with the new requirements around deletion we had from our regulators—both the FTC in the US and the Office of the Data Protection Commissioner in Ireland. That has been a very significant project for us, with extensive resources deployed. That is for all our users, and this is for a subset of our users in a very specific way, just for the UK authorities. It is not the kind of project that we have ever done before, so it would be a major undertaking just to set it up. Then there would substantial ongoing costs to ensure that we continued to comply not just with this law but with all the other laws in the penumbra of this. We have to ensure that we do not breach those laws because of what we are doing very specifically for the UK Government.

Colin Crowell: I would agree as well that it is impossible for us to predict the costs overall or the costs for Twitter because we do not know the extent of this or how sweeping the requests would be on us. The other points that Mr Collins and Mr Milner made are absolutely true: the volume of traffic over time is continuing to increase on the internet. We know this first-hand. Twitter is six and a half years old. It took three years and two months to go from the very first Tweet to the billionth Tweet. We now serve a billion Tweets every two and a half days. The volume over time will increase, so I do not know what the collection of that volume of data and the ability of people to sift through it adequately would cost, and I do not know how they would make the filtering aspects work.

Q655 The Chairman: Could I ask each of you to consider sending us a note on all cost aspects, not relating to your individual companies—we do not want that detail—but the items that could incur cost. Mr Collins has run through some of those, as has Mr Milner. We will not publish that but we will ask it from others as well. It would be helpful to the Committee to have from you and others who have given evidence your views on the things that might cost. We can collect that, make it anonymous and send it to the Home Office to say, “Look, these are the costs that various companies think they might incur if they were to do this”. I would be very grateful if you could do that. I do not think we are asking you to breach any confidences there.

Simon Milner: So you want the cost headings.

The Chairman: Yes. Do not try to put your own figures to them. Just say, “If we were to do this, these are the cost headings we would incur”. That might be training, extra lawyers, storage, data farms and the whole shooting match. Any other questions from colleagues?

Q656 Stephen Mosley: Trying to be positive about the Bill, with Facebook and Twitter, it looks as though people would have to store their data. If the Bill goes through and it happens, is there anything that you would suggest could be done to make it easier on you and on the British Government to make the system work?
Simon Milner: I am afraid not. As I have said, we can see only great complexity and extensive cost for minimal benefit. I would always want to be helpful but I am afraid I struggle to see how you can make this Bill more palatable.

Steven Murdoch: I agree. There is nothing that can really be done from our perspective. Either it would not apply to Tor or be used for Tor, in which case it does not make a difference either positively or negatively, or, if it applied to third parties for collecting Tor data, then we would have to have some way of preserving the safety of our users, and that would probably involve the users who choose to send data over the Tor network bypassing the UK. That would not affect users of the Tor network who were based in the UK.

Colin Crowell: I would just go back to a point I made earlier: it is Twitter’s policy to preserve evidence once we are informed by law enforcement that they are seeking it. Regardless of what our data retention policies might be for various types of non-public data that we may have, once we are informed by law enforcement that they want information for a particular account for a case that they are building, it is our policy to preserve that evidence until they go through the legal process to obtain it. Again, finding some technological means to capture all of our data, including on users who will never commit any crime, to deal with the very few instances when law enforcement look for our non-public data to be conveyed to them as part of an investigation seems to us like overkill.

Simon Milner: To reiterate, that does not mean we think that there are no ways of improving the processes between ourselves and law enforcement. If you want to spend £2 billion of public money, though, why not use it to improve the intergovernmental MLAT process, which is a very important part of this whole regime? You could spend a fraction of that money on significantly improving that process and really help law enforcement.

Q657 The Chairman: It has also been suggested to us that our police officers or security officers in the agencies should be better trained to ask for the right information, as the existing regime has all the information there but we ain’t asking for it correctly. Do you agree with that?

Simon Milner: Absolutely. Indeed, that is why we spend time educating police officers on the process for seeking data from Facebook. We have published guidelines and an online mechanism for them to ask for data, based on them being authorised to do so. My colleagues recently spent some time in Glasgow meeting a large number of UK police officers and informing them about the process in place to submit a request for data from Facebook.

Q658 The Chairman: And was the end result that they were amazed that that ability was there?

Simon Milner: Some of them were used to it. It is like many things, though: it is having someone there putting a face to Facebook, who can help them to understand how to use the system. Actually, the UK is very good and has a good system. Most agencies know how to use our system and have well trained officers for that purpose. The UK is ahead of the pack in this area.

Q659 The Chairman: Is it the panel’s view—I do not want to put words in your mouths—that part of this 25% gap, whatever it might be, might be closed with better training and more sophisticated techniques in the police and security services?
Stephen Collins: If only half the £1.8 billion was spent on training, that would be money well spent.

The Chairman: Thank you very much, gentlemen, and your supporting teams behind you, for coming here today. This has been very, very helpful. I am not just saying that; it has helped us. It has given us information that some of us may have suspected before but you have spelt it out for us. As I say, we will have a transcript that we will share with you, and we will discuss with you whether we would be able to use any of it, in an anonymised version or otherwise, in our published evidence. However, we are not going to expose you, having made a commitment that we will keep this confidential. If we could use some of it with your agreement, though, that would be helpful; if we suddenly come to conclusion X based on what you have said, it is helpful if we can publish some of the evidence to justify that. Please also supply the information on the discussions that you have had with the Home Office—the gaps and the worries that you have, the questions that would like us to ask—and any of the training that you could do. Thank you once again.
TUESDAY 16 OCTOBER 2012

Members present

Lord Blencathra (Chairman)
Lord Armstrong of Ilminster
Baroness Cohen of Pimlico
Lord Faulks
Lord Jones
Lord Strasburger
Mr Nicholas Brown
Michael Ellis
Dr Julian Huppert
Stephen Mosley
David Wright

Interception of Communications Commission [Sir Paul Kennedy and Joanna Cavan] (QQ 660-690)

Examination of Witnesses

Sir Paul Kennedy, Interception of Communications Commissioner, Interception of Communications Commission, and Joanna Cavan, Chief Inspector, Interception of Communications Commission

Q660 The Chairman: Welcome to our public evidence sessions. Welcome to Sir Paul and your colleague. I am sorry you were kept waiting. We were just about ready to start at 3 pm when a vote occurred in the Commons. We are likely to be interrupted throughout the day with votes in the Commons and Lords as well. I am sorry about that but that is the price we pay for living in our wonderful democracy. Before we start with questions, Sir Paul, could I ask you to briefly introduce both of yourselves for the record?

Sir Paul Kennedy: I am the Interception of Communications Commissioner, and have been so since 2006, so I have done something over six years in that office. My colleague is the chief inspector, who works under me with a team of five inspectors under her, and perhaps I can explain—if you permit me to do so—the way in which our work divides.

I in fact have two parts to my role. One is the oversight of interception, and I am sure that you are all sufficiently familiar now to know the difference between interception and data. Interception is that part of the activity that is covered by chapter 1 of part 1 of RIPA. I do that myself, so that my function is to check that the Secretary of State who grants a warrant has done so on grounds that are sustainable. It is an auditing function carried out after the event and I do it. I also have an oversight role in relation to data. Data of course is not the content, it is the context—if I can put it that way—of any communication.

As you know, there are a large number of occasions when data is obtained, and it would be physically impossible for me to do them all anyway. So that side of my functioning, in other
words the oversight of data, is carried out on my behalf by Ms Cavan and her team of inspectors, and that is how our functions relate. In the early days of my activity I did do a couple of inspections on her side of the fence so that I understood what was going on, but in reality I do not normally see anything other than the reports that her team produces, and they are incorporated into my annual report. I hope that is helpful and explains our two different functions.

**The Chairman:** It is very helpful, Sir Paul, and thank you for that opening statement. Could I ask Lord Armstrong to ask the first question, please?

**Q661 Lord Armstrong of Ilminster:** Sir Paul, you said in your written evidence that a strong case has been made that without the draft Bill there will be a declining capability. I wondered if you could tell us what was the evidence, in more detail, that persuaded you to take that view.

**Sir Paul Kennedy:** It is quite difficult to give you specific examples without crossing a line that I could not do in a public forum. I think you already have the evidence from others that over the last few years what has happened is that there has been a decreasing amount of the information that an investigator—if I can put it that way—either on the counterterrorism side or on the domestic policing side, requires being available. It has never been available 100%. That is a myth. You have not always been able to get everything you wanted, but the amount that you cannot get has increased and it has now reached the position where it is said about 75% of what you need you can obtain, and the figure is falling, and within a couple of years it will be down to about two-thirds of what you need. If you think of it that coincides with what we all know from our personal experience. When I started to do this job—only six years ago—people who were engaged in illicit activity communicated probably by mobile phone. They now communicate much more frequently by internet protocol, and they can do so without leaving anything like as great as a footprint and sometimes no footprint at all, and it is in order to meet that increasing risk that, it seems to me, the main thrust of this Bill is an essential step for Parliament to take. Does that answer?

**Lord Armstrong of Ilminster:** Yes, thank you very much.

**Q662 Lord Jones:** Sir Paul, I am to ask my question on behalf of the Chairman and the Committee.

**Sir Paul Kennedy:** Yes.

**Lord Jones:** It is like All Gaul: it is in three parts. May I proceed? When your inspectors randomly sample the applications put forward by large users of communications data, what percentage of applications do they inspect? Then, how many of the 494,000 requests made in 2011 did the IOCC team inspect? And thirdly, are you satisfied random sampling gives a reliable picture of each authority?

**Sir Paul Kennedy:** Can I first of all put aside the small users because, not surprisingly, 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. That accounts for a percentage, but a small percentage, of the total figure you have just been talking about. The remainder, about 488,505, are the big users. Different considerations apply, and I think it is important to have this in mind also. Someone like the Metropolitan Police have a trained team of what, in the jargon are called SPOCs—single point of contact officers—and therefore
you are dealing with a sophisticated arrangement. By contrast, the small users, for example the local authority, have not done one for two years and they have quite a difficulty in knowing how to do it right, so one starts from that perspective.

The next thing that I would like to stress is that there is a difference between requests, which is the 488,500-odd, and applications. That is not easy to hold on to, to begin with. In order to acquire data you must make an application. The application may immediately generate several requests; different telephone numbers, if I can put it that way. Because the statistics are not complete across the board, we do not at the moment have easily accessible the numbers of applications, but an inquiry was done by Ms Cavan to try and see what the relationship was. It was not a particularly prolonged inquiry. It was only conducted over a limited period, but it looks as though you might say that each application gives rise to at least two requests so you need to bring the numbers down. If you do that, and then you look at the number of applications that were inspected by the team, the answer comes out to, in round figures, about 10%. That answers the first part of the question satisfactorily, I hope?

Lord Jones: Thank you, Sir Paul.

Sir Paul Kennedy: That seems to us to be a reasonably sensible level. If you think of it in terms of auditing, perhaps in the accountancy world it is a reasonable level at which to operate. Now does that give one a fair picture?

There are other riders we have to attach to this. The first is that an application itself, when you are looking at it, may disclose an error of procedure—not often, happily, but it does. If that happens in the context, for instance, of a large police force, the next question of the inspector will be, “Have you been doing this all of the time? Let us see the other ones”. So there is the spillover effect. So the actual figure that has been inspected is not, as it were, tunnel vision; you will find the bits to the side as you go along. Because you are there for a day or two days doing an inspection, you get a pretty good feel of whether this team is working well or is not working well, and it is not surprising that when you go back 18 months later—and I have been in post long enough to see the reports in relation to all of this—normally speaking, those who have it right will go on being able to get it right, unless, for example, there has been a change of staff or something of that kind, or the computer system has been playing up or something of that kind. So I think the answer is—if I have remembered all the legs of the question—so far as the first, put in bald figures: about 10%. Do we get a good feel as to whether or not the system is working well? Yes, I think we do, but only because you are there for quite a long time and systemic errors that are discovered hopefully are able to be corrected at the time when the investigation is taking place.

Lord Jones: I am grateful, and—

Sir Paul Kennedy: Do tell me if I have not covered everything.

Q663 Lord Jones: Colleagues will I am sure. But the annual report is helpful, and I see you have the chief inspector and then five inspectors.

Sir Paul Kennedy: Yes.

Lord Jones: Are you able to tell us how you acquire such people? What kind of people are they? How long are they with you?

---

1 Sir Paul Kennedy clarified the inquiry revealed an average of 3 requests per application.
Sir Paul Kennedy: Happily, they do not change jobs very often, which I am extremely grateful for, because they acquire expertise. Give your CV; can I ask her to give her CV?

Joanna Cavan: I have worked for the commissioner and the previous commissioner for nearly eight years now, and we do have quite a consistent team who have been supporting the commissioner for some time. I came from a private company where I worked as an independent expert witness in forensic telecommunications, and prior to that I worked for a police force. The majority—well, it is a split actually, half of my inspectors come from a police background where they are senior retired police officers and the others are civil servants, so we have a mixture of backgrounds.

Sir Paul Kennedy: The civil servant ones are mostly Customs.

Lord Jones: Would you take part in the selection of the inspectors?

Sir Paul Kennedy: Yes. I took part in the promotion of this one because she succeeded her predecessor, and I think I took part in the last appointment we did too, so yes, I do. We advertise within a fairly confined area. Obviously we do not go to the national press, I do not think, on this but we advertise in Civil Service periodicals and police periodicals and so forth, when a vacancy occurs. You need to have—and I have seen this in other walks of life—people who have a certain degree of competence obviously, but who are available to do this kind of work usually because they have ceased to do something else. In reality, senior police officers or senior Customs officers who are just on the point of retirement are the sort of people who tend to be interested in this kind of work. From our point of view, it seems to me that they are useful people to have on board because very often they have used material at the other end and they have had experience of how the systems do work or ought to work, so they need less training and are more alive to the work we are doing than they would be if they came cold from the public.

Q664 Lord Jones: Lastly from me, Sir Paul, may I ask you: how often does somebody like you see the Home Secretary, and have you seen the Home Secretary—this one—to discuss this draft Bill?

Sir Paul Kennedy: No, is the answer to the second question. I see the Home Secretary normally once a year and—this is my other role, in relation to the warrant-signing Secretaries of State—I see all the warrant-signing Secretaries of State on an annual basis. If I need to see any of them for a specific purpose, then I ask to see them but, in fact, normally I see them on an annual basis.

Lord Jones: Thank you.

Q665 Lord Strasburger: I would just like to return to the first question for a moment. I did not get a chance initially. You stated that there is a capability gap of 25%, rising to 35%. Is that your own assessment or is that one that you have heard elsewhere?

Sir Paul Kennedy: No. I do not have the facilities to give my own assessment in that way, but I know from what I hear. In all the agencies I visit—and I do visit them quite regularly in the course of my work—they tell me, “We weren’t able to progress that any further because we cannot get that data”, and that is an increasing problem for all of them. So I do not measure it. I cannot measure it.

Lord Strasburger: The figures of 25% to 35%; you were repeating what—

Sir Paul Kennedy: What you see in the papers you have yourselves.
Lord Strasburger: —I presume the Home Office said?

Sir Paul Kennedy: Yes, who gather it from the agencies.

Lord Strasburger: Thank you.

Q666 Mr Brown: Have you tested the labour market more broadly for senior operating staff, and are you not worried—I understand your reasons and I think you have put them very well—that you might be drawing your staff from too narrow a base and that there might be a breadth of experience that you are not drawing on?

Sir Paul Kennedy: We have not tested the labour market more widely, no. On the other hand, I am not troubled about the base. If I can put it to you this way, if you saw some of the reports they produce when they are being critical of a police force, and they themselves were police officers, you would not have any worries. It is quite clear that they understand exactly what they are there to do.

Mr Brown: If it is any comfort to you, the police said something similar when they were here.

Q667 The Chairman: Sir Paul, can I just follow up as well on your first answer to Lord Armstrong and Lord Strasburger, on the capability gap? You have said you have seen in your six years the change from mobile phones to other means of communication. We have also heard a lot of evidence from others before this Committee to say, “If you looked at my mobile phone in the year 2000 you would get fairly bare bits of information from it. If you look at a modern mobile phone these days you will get thousands of extra bits of information, of websites and so on”, so the overall amount of information has gone up exponentially. How does that relate to the so-called gap?

Sir Paul Kennedy: I agree with what you, my Lord Chairman, have just put to me, that the amount of information capable of being taken is greater. On the other hand, if a mobile phone is serviced by a provider who has no personal business to keep the records, you cannot get anything because you are not getting into it at all. That is the real problem, that for very understandable reasons six years ago every provider, I think I am right in saying, in the marketplace had a business reason for keeping their own records, and it was those records, particularly in retrospect, that one was able to tap. If you were doing an inquiry in relation to a murder, you would be able to look for the records of the mobile phone that was found in the possession of the suspect, and what they had been doing at the critical times. Now the situation has moved on to a position where that provider simply says, “I have no records at all. I had no business reason to keep them. He pays me so much because he buys the phone and he buys a certain amount of time, or he has a contract that I do not have to keep any records of”, and the inquiry is at an end. If the provider is abroad—and this is an increasingly international market—the problem then is of the same dimensions.

The Chairman: I understand.

Q668 Dr Huppert: Sir Paul, how do your investigators judge what is a justifiable level of intrusion for communications data? When you are looking at the records, what are you looking for? How much information can you get to assure yourself?

Sir Paul Kennedy: What is a justifiable level of intrusion?

Dr Huppert: Yes.
**Sir Paul Kennedy:** I think you have to look at it on a case-by-case basis. There is no way in which you can say some formula will work across the field, but you look at necessity and proportionality in relation to any given application. On the ground—I think I can say hand on heart—it is not that difficult when I see what is in the reports and, performing my other role, I see what is put to the Secretary of State in an application for a warrant. It is perfectly easy to see. There are not that many that are near the borderline. There are a few.

**Dr Huppert:** So you look at the reports of 50,000 assessments and you think that they are all relatively easy to tell? That is your—

**Sir Paul Kennedy:** No, I am looking at the report of the ones that have been inspected by my inspectorate.

**Dr Huppert:** Which is a 10th of the whole data?

**Sir Paul Kennedy:** Yes. They are recording what they find. They are normally more addressing the procedure being properly operated. They will be looking at the individual cases. The report will be dealing with the satisfactory nature of the procedure. Of course, if there is an inappropriate application then it would come into the report. I do not pretend that the report is a reflection of every piece of paper they have looked at. Well, I take that back. They do not look at pieces of paper at all. This is all electronic. But of every application they have looked at, it will only highlight occasional ones, I agree.

**Dr Huppert:** According to your last report, your inspectors found 100 errors, or was it 99?

**Sir Paul Kennedy:** Yes, 99.

**Dr Huppert:** So there are some errors that are reported to your office automatically, but 99 you found by looking at a 10th of the data?

**Sir Paul Kennedy:** In fact, 77 of them, I think I am right, were local authority ones, and as we inspect 100% of the local authority ones you can take it those are all the local authority ones. So it is only the remaining 22 that come from the rest of the field, but 22 is 22 too many, I do not disagree. Very often, or nearly always, they are procedural errors. The sort of thing that we have found—I think I am right in saying off the top of my head—is the wrong level of persons signing the authority. In the police it is quite easy because an identified rank is established, but in, for example, local authorities there was no necessarily equivalent rank and it was signed at the wrong level. That is an error and it should not have happened, but it is not one that causes me to feel great anxiety.

**Dr Huppert:** But it would presumably mean that the evidence could not be used in a court?

Certainly, if the wrong rank of police officer gives an instruction, whether it has to be an inspector or higher and it is somebody lower, that is not a valid thing in court, so presumably any of those glitches would mean that that evidence could not be used in a court, is that right?

**Sir Paul Kennedy:** It may or may not be right. It depends on the context. It is a ground for raising it in court. On what the judicial ruling would be as to the admissibility of the evidence, I would prefer to be sitting as a judge before I answer the question.

**Q669 Dr Huppert:** There are different rules for different data types. We have talked about content as one thing, use, traffic and subscribers—

**Sir Paul Kennedy:** That is a very important aspect of what you have just raised a moment ago, that the vast majority of applications—and I am sure you will appreciate this already in relation to data—are what one might call telephone book applications. They are to find out
who was associated with this number. For many of the bodies who have powers, they only have power to get that kind of information, which is subscriber data.

**Dr Huppert:** Sir Paul, I think we are familiar with the breakdown but the definition, which I am sure you are familiar with, for subscriber data is, “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”. So presumably that means if I have an e-mail account that is organised by the University of Cambridge, as in fact I do, then subscriber data is not just the reverse directory you look up, which you have talked about, it would also include any information that the University of Cambridge holds on me, is that correct?

**Sir Paul Kennedy:** On the definition, it is. I cannot remember it ever actually being, in practice, a situation I have looked at, but yes.

**Dr Huppert:** So if the university held my medical records from when I was a student, which again it does, that would count as subscriber data according to what this says, because it would be information held or obtained by a person providing a telecommunication service about me?

**Sir Paul Kennedy:** I would like to think about that one. I am not sure.

**Dr Huppert:** This has been raised to us as a very serious concern because it is very broadly written. If you could write back to us that might be helpful. Subscriber data in the current Bill is page 63—

**Sir Paul Kennedy:** In the current—sorry?

**Dr Huppert:** In the current draft it is page 63, section 5. It is very broadly written and allows far more than the directory look-ups I think you are identifying.

**Sir Paul Kennedy:** Page 65?

**Dr Huppert:** Page 63, but if you want to write back to us I think that might be more useful than—

**Sir Paul Kennedy:** Sorry?

**Dr Huppert:** If you want to write to us about that I think that might be more useful than an immediate response.

**Sir Paul Kennedy:** As I understand it, what you are seeking is whether I am satisfied that the subscriber data is sufficiently narrowly defined. Have you an alternative to put?

**Dr Huppert:** One could define it in some sense as a reverse directory look-up whereas this allows any information held to count as subscriber data. If you look at the information that Facebook would hold on me, that Google would hold on me, it is very significant, and it is not at all clear here what that definition is. I hope that you are clear when you are doing inspections because, as you say, subscriber data is a lower level of authorisation.

**Sir Paul Kennedy:** Oh yes. In fact, that is what it is in reality. The width of the definition is not a point that has ever actually been a materiality so far that I can remember.

**Q670 Dr Huppert:** Can I then move on, because one of the things we have had a lot of concern about is how broad some of the investigations are? There is a big difference between a police officer asking for information on a particular phone and asking for very general information—that may be a cell dump, it may be collecting data from a mobile phone provider for every client for the last two weeks or something like that.

**Sir Paul Kennedy:** Every?
Dr Huppert: Every user, where were they in the last two weeks. One can imagine something very, very broad. Do you do anything systematically—

Sir Paul Kennedy: I do not see how that would possibly satisfy any of the existing tests. It could not be proportional.

Dr Huppert: I would tend to agree, Sir Paul, but reality does not always fit with what is actually proportional. But do you do anything to systematically look for phishing attempts?

Sir Paul Kennedy: Yes.

Dr Huppert: Do make sure they are individually checked, and how do you do that if you are only looking at a sample of requests?

Sir Paul Kennedy: No, that is probably something that I ought to go into a little bit more deeply. The nature of an inspection does focus on various aspects and, for instance, if there is a cell dump they would be looked at automatically as part of the inspection. If I can break it down, the way in which the inspections operate is you start with a random sample from the record of whichever police force it is. You then take a random sample of the data that that police force has asked for from the service providers, so that you get a back check. If I can put it this way, you go to Vodafone and you say, “How many requests have you had? Give us the number in the last 12 months from Cambridgeshire”, and we will select a few of those. Then when you go to Cambridgeshire you say, “Produce the files in relation to those”, so that is a back check.

Q671 David Wright: On that point, would you take a specific incident, outside of your random sampling, and investigate that incident? For example, a specific terrorist incident within the UK, would you actually look at that particular incident and the communications data used on it?

Sir Paul Kennedy: I think in reality almost certainly, because if you inspected that police force you would be looking at a big incident of that kind. Life is like that. They would want to show it to you and you would want to look at it, so yes. In every inspection, or pretty well every inspection I can think of—and we are rather focusing on police forces—they do produce examples of a particular operation and how the acquisition of data worked in relation to that operation. So, yes, they come very often as an appendix to the report on that police force.

David Wright: Earlier you said that you would use your judgment as to what was reasonable because each case was almost standalone in its conduct.

Sir Paul Kennedy: The person who uses the judgment in the first instance is not me. We are doing it retrospectively.

David Wright: Help us to understand how that process works then.

Sir Paul Kennedy: What you do is you look at the information you have obtained and decide whether, in those circumstances, it was reasonable to use the statutory powers—it was necessary and proportionate to do so. Given a particular set of facts, I do not think it is a difficult operation.

Q672 The Chairman: Sir Paul, can I move on to the possible extension of your powers if this draft Bill becomes law?

Sir Paul Kennedy: Yes.

The Chairman: In your written evidence you state you do not know how much extra work it will entail and how often you will need to inspect the CSPs, how many CSPs will be affected by
the draft Bill, and so on. Are you concerned that at this stage you have not been given enough information by the Home Office about the potential extension of your responsibilities?

_Sir Paul Kennedy:_ May I say, first of all, this is in fact not going to be me because my term of office ends at the end of this calendar year, but I will pretend that it is me.

_The Chairman:_ Well, the office of commissioner.

_Sir Paul Kennedy:_ The office of commissioner goes on. I am in no way critical of the amount of information that we have so far been receiving, because the Home Office has kept us in touch with these matters as they have developed. I think it is very much an area where we will have to learn by experience and I have had specific assurances that what we need we will have. So far as the first of the additional duties are concerned, I think that is probably one that can be dealt with by the chief inspector and her team of inspectors. 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. At the moment to say we ought to be going to the market for it, I think, is premature. I think until we see exactly what is required it is too early to do so. Furthermore, the way in which the Bill operates, as I understand it, is that an order would be made by the Secretary of State in relation to a particular provider. It would be at that stage that one would be looking about the operation of the Bill as a whole. Therefore, I think there is time, and it would be better if the time was used and the recruitment when it takes place was focused and appropriate. So I am satisfied we are being kept up to date, yes. Are we going to need more help? Yes.

_The Chairman:_ I should have asked Mr Ellis to come in at that point, and I intervened by mistake. Mr Ellis, if you wish to continue in this line?

**Q673 Michael Ellis:** Just briefly, Lord Blencathra. Sir Paul, as far as the whole extension of your powers is concerned, do you have any idea as to when you might get these details from the Home Office?

_Sir Paul Kennedy:_ In one sense, no, but I hope—

_Michael Ellis:_ You are quite relaxed about it, though?

_Sir Paul Kennedy:_ I am relaxed about it because I do not think we should try and jump the gun.

_Michael Ellis:_ How much time will you need to recruit new staff? Do you anticipate needing new staff?

_Sir Paul Kennedy:_ Probably not in large numbers, but probably the answer is yes. How much time do you need? It depends on the answer to the previous question, does it not? If we are dealing with people who are technically qualified, are we going to recruit them on a full-time basis or are we going to recruit them, for example, on a consultancy basis? If we need to get somebody on a full-time basis, three to six months.

_Michael Ellis:_ Do you engage your current staff on a full-time basis?

_Sir Paul Kennedy:_ Yes.
Michael Ellis: Are you confident that your current staff have the expertise required to take on the new responsibilities?

Sir Paul Kennedy: I think I have already answered that. In relation to the first section, from what I know of the Bill so far, yes. In relation to the filtering section, not necessarily. Probably not. I would not have, so I do not expect them to have.

Michael Ellis: You would have an idea of where to find them?

Sir Paul Kennedy: I think when I see what the filter involves I might have to take advice from people technically qualified within the Home Office as to where we should be looking. But my present impression is that which I have already indicated, that people who have IT qualifications are probably the ones we will be looking at but within that very broad field, a precise area to target, I do not know.

Michael Ellis: They will be vetted individuals?

Sir Paul Kennedy: They will have to be, unless they are already in the service. This is how sometimes one is lucky enough to recruit people who already have been vetted. But you are quite right, that is another timescale.

Michael Ellis: Do you currently ever see applications for communications data made by public authorities?

Sir Paul Kennedy: Yes.

Michael Ellis: Is that through the mutual legal assistance process?

Sir Paul Kennedy: No. We do not involve the mutual legal assistance process at all. That is controlled by the courts and we have had no hand in that at all.

Michael Ellis: Do you have any observations about how that works?

Sir Paul Kennedy: It is slow.

Michael Ellis: Slow—does that mean inefficient?

Sir Paul Kennedy: I think I know as much as you do, in the sense that I see what the timescale is in relation to matters that have gone through that route. I am not prepared to say it is inefficient. It would be wholly unsatisfactory to make a criticism of that kind without having been involved in investigating it properly.

Michael Ellis: So you are generally confident, though, that when furnished with the information that you require, your successor will be able to deal with the issues appertaining to staff and facilities appropriately?

Sir Paul Kennedy: Yes, I think so. It required an assurance, which I have had from the Home Office, that essentially if I or my successor goes and says I need another member of staff they will have it. That assurance has been given.

Michael Ellis: In your six years, have you made such requests previously?

Sir Paul Kennedy: For increases in staff?

Michael Ellis: Yes, or equipment or facilities or anything along those lines. You have?

Sir Paul Kennedy: Not to a great extent, but to a limited extent, yes.

Michael Ellis: You have not met with any obstruction or difficulties?

Sir Paul Kennedy: No.

Q674 Michael Ellis: So, just to take a step back if I may, just on the need for this draft Bill, you are coming up to the end of your distinguished term in this position. I think you say you finish at the end of the calendar year, is that right, Sir Paul?

Sir Paul Kennedy: Yes.
Michael Ellis: If one was to invite you to make a brief appraisal of your six years in the position and how you see things going forward perhaps in the next six years, are you satisfied, in all the circumstances, that this is a necessary measure that is both proportionate and also meets the challenge presented by criminals and terrorists and other wrongdoers going forward?

Sir Paul Kennedy: Absolutely, is the short answer. I have no reason to doubt—indeed, this is where we began—the figures that I have been given as to the extent to which the ability to obtain information has been contracting. I regard that as potentially very dangerous, and it means that we are unsighted in a section of the market, and we are in a world that is still extremely volatile. It seems to me that, against that background, what is now being sought is not to increase the amount of information available in the public domain principally, it is to require service providers to retain certain information that can only be accessed in a proper way—that is to say, when it is shown to be necessary and proportionate to access it. Then it can be used not only for the purposes of securing convictions—one tends to forget because that is the side we can talk about—but also by the intelligence services for disruption. Disruption is a hugely important part of the safety that we all enjoy. A lot of it is never even mentioned but, in fact, if they lose the capacity in that direction, and you lose the capacity to detect crimes that have been committed, to the extent of which could be something in the region of 20%—one in five of the pieces of information you want—that is very serious and we should not be doing that, either for our own safety or the safety of our children.

Q675 Lord Strasburger: Sir Paul, this draft Bill will add a very large amount of data, on top of the data that is currently covered by RIPA, and therefore this Committee is concerned to be comfortable that the auditing of RIPA is going well and, secondly, we are concerned to know how well the public authorities are complying with the law. I have read your 2011 report very carefully. It is quite long on enthusiasm for the benefits of communications data but it is quite short on the details of your inspections. As an example, on page 33 and page 44 there are two graphics that show the level of compliance for two groups of public authorities. You have grouped them into good, satisfactory and poor, but I have no idea how good the public authority has to be to be good. What percentage of compliance does a public authority need to achieve to reach your category of “good”, and equally for “satisfactory” and “poor”?

Sir Paul Kennedy: We tried to make an overall evaluation of the reports in the way we put the message across. If you read the remainder of the text around the graph, you realise how they have come into existence. The vast majority of police forces and law enforcement agencies had fully implemented the previous recommendations. When the inspectors go they make recommendations, and if they implement previous recommendations then you get to a situation where their performance is of a level that you expect to be good. If at the time of inspection you find that they are not complying with the Act in certain respects, it may be a minor error, it may be all right but not very good, it may be simply awful, and we have tried to make those distinctions in those bar charts. I do not know how much more we could do that would be of help, but if we could we will certainly try.

Lord Strasburger: In order to get into your “good” category, does that mean 100% of requests were compliant, for example?

Sir Paul Kennedy: Yes, in most cases. Yes. The 72% is not a 72% good. It is 72% saying you are an efficient authority.
Lord Strasburger: Yes, but what does “good” mean? I am still trying to find out what “good” means. Is it 100% compliant, 80%, 90%? I am trying to get a handle on how many—

Sir Paul Kennedy: It means that if you go to a police force and there is very little, if anything, wrong with the way in which they are using their statutory powers you class them as “good”.

Lord Strasburger: What is the level for “satisfactory” then?

Sir Paul Kennedy: The level of “satisfactory” is not as good. It is the next level down. It is that they are not as good as that. They in fact have some errors, but overall they are doing it quite well—satisfactory.

Lord Strasburger: How many errors is “satisfactory”??

Sir Paul Kennedy: If you ask me in relation to a particular police force I will go and look it up, but I am sorry—this is marking all over the world. It is like academic marking. You have good ones and satisfactory ones and poor ones.

Lord Strasburger: In order to get a grade in my GCSEs, I will know that to get grade A I have to achieve 72%?

Sir Paul Kennedy: Yes.

Lord Strasburger: What does a public authority have to achieve to become good or satisfactory or how bad does it have to be to be poor?

Sir Paul Kennedy: I am sorry, but if there are a lot of errors then it is poor. If there are only one or two errors, it depends on the quality of the error. If the error is significant, and there are two or three of them then they may be poor although there are only two or three errors. If there are two or three errors but they are not very serious errors they may still be satisfactory. I cannot do any better than that without referring to a particular report.

Lord Strasburger: You are telling me that it is a totally subjective judgment?

Sir Paul Kennedy: It is not a subjective judgment. It is a judgment made on the basis of carefully prepared reports, and I suspect you would support it if you read the report.

Lord Strasburger: Perhaps, Lord Chairman, if I could possibly come in here and just add some context? The “good”, “satisfactory” and “poor” ratings come out of the recommendations, and this year for the first year we have disclosed the traffic light system that we use for recommendations. The recommendations are made across very distinct areas. We have set inspection baselines, so when you talked about “in your GCSEs you have to hit certain marks in certain areas”, we have a very structured inspection baseline document that covers the application process, the authorisation process, the urgent oral process, the content of authorisations and notices that goes to the service providers, on the quality of those. We inspect a number of baselines that come directly from the acting code of practice, and we mark the public authority against those baselines. If we then make a recommendation against one of those baselines, if it is a very serious compliance issue that has caused breaches or potentially data has not been acquired in accordance with the law, that will be given a red compliance recommendation. It is very unlikely then that that public authority would get a good grading overall if they have some red serious compliance recommendations.

What we wanted is, if we give a public authority 13 recommendations, it was very difficult for them to decide which ones to hit first, which ones were perhaps more serious compliance issues that they needed to address, so that is why we introduced the traffic light system that shows the severity of each recommendation against each baseline. Then a chief officer is able to say, “Okay, in this area we have really serious poor compliance. We have red
recommendations so we need to address those”. So once we see the number of recommendations, the colours of those recommendations, which represent how serious the compliance is, we will then use those quantitative results to move them into either a “good”, a “satisfactory” or a “poor” category. Those who have ended up with a “good” overall will have mainly green recommendations that are more around efficiency and effectiveness, whereas those who have been given a “poor” rating will have recommendations around the red category, which are serious compliance issues. I hope that helps.

**Lord Strasburger:** So the ratings are about process—how well they are applying the process? They do not give me any indication of how many times public authorities are not complying with the procedures or are making requests that are not compliant.

**Joanna Cavan:** They will include that, because if a public authority has made a request that is not compliant, that will automatically be a red compliance issue.

**Lord Strasburger:** How can I find out how often this happens?

**Joanna Cavan:** We will report on the serious cases in the annual report. It is very difficult to report on all cases we find because of sub judice, so we cannot report on absolutely everything openly. But they will be mentioned in the report where we have found serious non-compliance issues.

**Lord Strasburger:** I am just after statistics, that is all, I am not after the details.

**The Chairman:** Would you possibly be able to send those to us?

**Joanna Cavan:** I could certainly have a look at that for you. Of course.

**The Chairman:** Yes, please. That would be helpful.

**Q676 Stephen Mosley:** When you are looking at the compliance do you look at the technical systems used by the public authorities, or do you rely on the paperwork that you are supplied and the recommendations that you are supplied from those authorities?

**Sir Paul Kennedy:** The answer is there is no paper. The answer is you look at the base material.

**Stephen Mosley:** So you go in there and you look at their technical systems and make a decision based on that for a public authority.

**Sir Paul Kennedy:** Yes.

**Stephen Mosley:** What about with a CSP?

**Sir Paul Kennedy:** Sorry?

**Stephen Mosley:** What happens with a communications service provider that might not be a public body?

**Sir Paul Kennedy:** I do not have any role in relation to communications service providers. I do see them and I visit them, but I do not have a statutory obligation to do anything with them, other than talk to them and see that they are getting the service they need from the other end. I cannot go to them and say, “Produce to me your records”. I have no statutory warrant to do so. In this Bill, there is a certain role in relation to communications service providers. There was not previously. But, for what it is worth, I have always gone not to all of them but to the large providers, in order to talk to them about what they do and to make sure that the relationship they have with, for example, agencies is a satisfactory one.

**Stephen Mosley:** Would you have a role at verifying the interception and communications data logging equipment that has been put on the CSPs’ networks?
Sir Paul Kennedy: As I understand it, that is part of what would now be envisaged, yes. We will know how this will work out on the ground when we know more of the technicalities.

Q677 Stephen Mosley: Going back to the public bodies, you say you currently have the right to go in there and verify their systems. From some of the evidence we have seen—and I know Big Brother Watch says this—people say that you might have the power to do it but there does not seem to be anything in your reports to say that you have actually been in and looked at the systems themselves, rather than relying on the evidence that they supply you. Have you ever used those powers to go in and look at their systems?

Sir Paul Kennedy: Yes.

Joanna Cavan: We do conduct the inspections on the systems, so nothing is printed out for us. We have log-ins to that public authority system and we conduct the inspections on the system. So we do a full audit trail and the action is taken on that system. We would not be able to do it on paper because we would not be able to see the audit trail, as the process works electronically, so if you were not examining it on the system it would not be robust enough.

Stephen Mosley: Moving to the new system, when you have the rights to do that with the CSPs as well, do you think those CSPs would be happy to allow you to have that authority to do it on their networks?

Sir Paul Kennedy: The degree of co-operation we have always had from the CSPs is very high. One of the basic factors is that in this country we pay the CSPs for their co-operation. I am not saying they make a great deal of money out of it but they do not lose money out of it and we do get very good co-operation. I have no reason to doubt that if this Bill were to become law that would continue. As I understand it—and it is quite important to make this point—the purpose of those who wish to see this Bill become law is not to use the powers enshrined in it, except when they have to. They want to obtain most of the material that they need to have, by means of co-operation. I think that the past suggests that that will be possible provided there is in place a statutory formula to be used if the co-operation is not forthcoming. That is why I think this Bill is very necessary.

The Chairman: Thank you very much, Sir Paul.

Q678 Baroness Cohen of Pimlico: I would like to ask you about the warrant system in relation to local authorities. It is quite a popular suggestion among some of the people who gave evidence to us that if you are a local authority and you want to access communications data you should get a warrant. I notice from your evidence that you are not at all convinced about this.

Sir Paul Kennedy: No.

Baroness Cohen of Pimlico: Would you like to tell us why you think the SPOC process beats a warrant?

Sir Paul Kennedy: One can tackle this question from the other end in a sense. I do not see any justification for making local authorities get a warrant if you are not going to make a police force get a warrant. You are dealing with the same type of material from the same source, and volume considerations, apart from anything else, suggest that that would be wholly unworkable if we introduced it in relation to 500,000 applications for information. If the system can be properly worked, as it is by some local authorities, for example, it provides a very high degree of safeguard. The applicant in the housing department, or wherever, or
market traders or something like that, has to make an application that goes to be considered by a senior member of staff not involved in that particular investigation, and he or she then gives the authority for it to go to the next stage.

The problem—and I have hinted at this already this afternoon—is that a number of local authorities do not use their powers very much, perhaps because they are not very big authorities or they do not have particular types of problems. When they come to use them they do not necessarily get the procedure right, and that causes problems. Happily, there is a thing called NAFN, the national association—you have probably heard about NAFN, and I have mentioned it. NAFN has established a central authority that they can use, and it is hugely efficient. We have inspected both of its sites more than once and it gets it right. Some 70% of local authorities now use NAFN and the number is rising. Should the others use it? For the most part, yes, but I am not going so far as to say that I think you should necessarily make it a statutory requirement to use it. What I would quite like is for it to be made easier to use. The ones who do not use it do so on financial grounds. They say, “It would cost us something to use NAFN”. If a formula could be devised that would take away that hurdle, I think that then the probability is they would use it too and the question would almost disappear, because there would be a satisfactory way of local authorities processing their applications, which would be every bit as good as MI5.

Baroness Cohen of Pimlico: I suppose the civil liberties argument is that you do not give powers to them that you do not feel that they really need.

Sir Paul Kennedy: Yes.

Baroness Cohen of Pimlico: You are perfectly comfortable in giving the police and security services powers, but you are saying that the procedures are in fact exercised in the same way.

Sir Paul Kennedy: Yes, 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 they perhaps 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.

Q679 The Chairman: When you say “local authorities”, you do not just mean local councils; you mean they are the public authorities.

Sir Paul Kennedy: Yes.

The Chairman: So, HMRC, the Fire Service, the Department of Health—those people.

Sir Paul Kennedy: HMRC is quite a big operator, so it comes on the other side of the fence. Some of the others, as you, Lord Chairman, said, like the fire service, are exactly on this side of the fence.

The Chairman: So the encouragement you wish to give to those others to move on to what in the Committee we nickname the “super SPOC system”, you would extend that out as far as—well, let us keep the security service out of it—the police, who are doing their own SPOC thing, HMRC possibly, but everyone else you would like to see covered by the super SPOC.

Sir Paul Kennedy: If you take out the intelligence services and the police, and HMRC—SOCA I envisage being part of the police—I would be perfectly happy with everyone else using NAFN. The problem of course is that an awful lot of them are not local authorities and NAFN is a local authority body, so something would have to be done. I do not think that is
impossible to enable the Mersey Docks and Harbour Board, or someone like that, to be able to use a body that is not theirs.

**The Chairman:** You think that would give a higher level of certainty, safety and accuracy than trying to use their own internal SPOC systems, or even a magistrate’s warrant.

**Sir Paul Kennedy:** Absolutely, yes. That would certainly be so other than with perhaps the very large authorities. The City of Birmingham, for example, as a large authority may have enough traffic to develop quite a degree of sophistication of its own.

**The Chairman:** What about the FSA?

**Sir Paul Kennedy:** The FSA has quite a lot, too. It is one of the biggest users.

**The Chairman:** Thank you, I found that very helpful.

---

**Q680 Dr Huppert:** Sir Paul, your submission suggests that you want to keep the number of permitted purposes that communications data can use. You will be aware it is a long list, from national security to any crime and to collecting any tax or duty, and so forth. Is that right that you want to keep all of that full list?

**Sir Paul Kennedy:** Yes. I do not see any reason for not keeping it. I am not wedded to this, but I think the reality is some of these are quite important even though they have not cropped up recently, if one can put it that way, yes.

**Dr Huppert:** You are presumably aware that Mick Creedon, who is the Chief Constable of Derbyshire Police and the ACPO lead on serious organised crime, commented—and I believe it is a direct quote—“If I am driving on the motorway and I see someone on a phone texting at 80 miles an hour, that for me would pass the test immediately”. He is technically right that it is a crime. Would you agree that that was a proportionate use of communications data?

**Sir Paul Kennedy:** I have hesitations about it. I agree. I read that, like you. But on the other hand I am doubtful about the serious crime frontier, if we are in that territory. It arises more particularly and more frequently in relation to local authorities. They have a statutory duty to investigate fly-tipping. It is easy when it does not affect you or me to say, “Not very important crime”, but if it affects you directly it is very important to you, and the only way in may be to find out who owns the mobile number on the card that was given to the householder.

**Q681 Dr Huppert:** Can I go back to your role of inspecting this? Let us say Mr Creedon authorised the use of communications data for somebody who was texting at 80 miles an hour. You then inspected that. Would you say, “This is perfectly legitimate, it is a crime. It is fine”? Would you raise questions about it? Would it fall into your category? Would it push the Derbyshire authority down towards “satisfactory” or “poor”? Would it have any effect at all?

**Sir Paul Kennedy:** It must depend entirely on context. There was a case on the M1—I cannot remember the name of the person who was involved. A child was killed, and you will remember it too probably, near Sheffield. The suspicion was that the driver had been on his mobile phone at the time when the accident occurred. Now that is a pretty serious matter, is it not?

**Dr Huppert:** Sir Paul, the example that Mr Creedon gave was quite clear, “If I am driving on the motorway and I see someone on a phone texting at 80 miles an hour”, there is no suggestion of anything else; it is just 80 miles an hour on a phone. He believes that would be proportionate. He would go ahead with it, presumably. What would happen when you inspected that authority? How would you look at that case? Would you flag it up as a concern?
Sir Paul Kennedy: I am being whispered to, so, Joanna?

Joanna Cavan: I do not think an application just on the basis of that one sentence, if that was all there was, would even reach the SPOC, and get through the SPOC, and it would not even go to a designated person to consider. In the robust guardian and gatekeeper role that the SPOC performs, they will be looking for certain tests to be met, and they are very professional and they take it very seriously. So if there was a lot more to that case, if it was dangerous driving and something happened and there was a lot more information, it could be that the communications data was required to prove that offence, but something just on the basis of that one sentence with no more detail, that would not—

Dr Huppert: Ms Cavan, you are hoping that the SPOC would say to their Chief Constable, “I am sorry, you are wrong, we are not doing this. I know you are the lead nationally for the police on this but I am not going ahead with it”. That may be the case. Let us say the SPOC did not feel comfortable enough to tell their Chief Constable that they were wrong and approved it, you would then inspect it and have a look. You would see this. What happens next?

Joanna Cavan: Then we would ask for any further information. Obviously an application form should stand on its own, so that should have contained everything it needed to to justify the tests. If we are not satisfied that there is enough information there we will ask to look at the case file. We will ask for the applicant, and the designated person who approved that request, to provide us with their thoughts and justifications, if there are any policy logs around the decisions that were made and the reasons why. So we will look at whether there is any more surrounding information or evidence, but ultimately if there is not we will conclude that we do not deem that request was necessary or proportionate.

Dr Huppert: I think that is very helpful given this disagreement there. So you would give him a chance to add to the information that was originally provided and to look back six months ago and say, “Actually, I think there was some other thing. I was very concerned about something else”? They would have that chance above what they asked authorisation for.

Joanna Cavan: Yes. I think it is really important because the quality of applications does vary and sometimes someone may not have put everything they needed into the application. Technically, that should not have gone all the way through if it is not of particularly good quality.

Dr Huppert: Would you flag it up that it was not of good quality, and that would again move people down the rankings?

Joanna Cavan: Yes. There are two areas. We will either conclude that the request was not justified or we will conclude that, on the basis of the information we have seen, the request was justified but it was not sufficiently outlined in the application on the case.

Q682 The Chairman: So you are making some judgment on proportionality. Would you like, Sir Paul, to see additional powers given to you on proportionality to make wider judgments?

Sir Paul Kennedy: I do not think so. The situation is entirely as has just been described to you. I think that in judging or reviewing other people’s judgment one has to keep that in mind also, that you are deciding whether or not the application was justified. You are not the first-instance decider. That is quite an important distinction to keep in mind. What has just been said, of course, is entirely true—that if the paperwork is not up to standard you certainly see what the paperwork was founded on. When you then look at what it was founded on you may
be able to say, “Well, even though it was not up to standard it was clearly a necessary and proportionate act to exercise the statutory powers”.

Q683 Mr Brown: Our constituents worry that information about them that ought to be confidential will be discovered and then improperly disclosed, and this could be everything from a public official with access finding out something about somebody they know, to public officials obtaining information on, say, a celebrity or a person in the public eye and selling it to the newspapers. We know these things happen. If people do such things, should they not be caught and punished?

Sir Paul Kennedy: Yes, it is a criminal offence to misuse the powers.

Mr Brown: I think the offence is misconduct in public office.

Sir Paul Kennedy: Yes. No difficulty about that proposition. I do not—

Mr Brown: How many such prosecutions are there?

Sir Paul Kennedy: Of misuse within our sphere?

Mr Brown: Yes.

Sir Paul Kennedy: As far as I know none. But if people are wanting to acquire information of that kind they do not use legal means, not normally.

Mr Brown: I understand that, but what the public are looking for is safeguards against that, and catching people and punishing them would be one safeguard.

Sir Paul Kennedy: As far as I am aware, there is no misuse of that kind within the area in which I operate. That there is misuse of that kind I know as well as you because I read my newspapers.

Mr Brown: I think the public’s fear is not so much in the area in which you operate but—

Sir Paul Kennedy: Legal intercept does not give rise to that type of conduct.

Mr Brown: No, but the information is being shared with others and then comes into the public domain. The route is not a direct one; it could be an indirect one.

Sir Paul Kennedy: I cannot immediately bring to mind any recent instance of information being leaked, which has been obtained for a proper purpose, if that is what you mean.

Mr Brown: If we were looking for a way to reassure our fellow citizens that the citizen was safeguarded against such an abuse, how should we go about it?

Sir Paul Kennedy: I have absolutely no doubt that, if that happened, there would be appropriate measures taken, probably in the form of a prosecution, yes.

Mr Brown: Do you think the courts would be supportive?

Sir Paul Kennedy: Yes. I do not think there is any difficulty. If you obtain information in the course of your duties under RIPA, and you disclose it to someone else, you are committing a criminal offence if you disclose it to somebody who should not have it. It is a matter of concern to people such as, for example, the IPCC, yes.

Mr Brown: Our fellow citizens are not reassured. That is just a common line.

Sir Paul Kennedy: The powers are there and they would be exercised.

Q684 Lord Strasburger: Sir Paul, on pages 42 and 43 of your report, you have identified two local authorities where 52 requests were not in accordance with the law. I would like to know, if you know, what penalties or sanctions were applied to the individuals or the authorities in those cases.

Sir Paul Kennedy: Sorry, what page?
Lord Strasburger: Page 42—the bottom of 42 and the top of 43, 52 requests not in accordance with the law. What happened to those individuals and those authorities?

Joanna Cavan: In those cases they obviously received poor compliance in those areas and the recommendations would be that, if they are going to take those cases to court, they should inform the prosecutor that that data has not been acquired in accordance with the law, and then that will be up to—

Lord Strasburger: But what happened to the people who failed to comply on a large scale?

Sir Paul Kennedy: We report to the person who is in charge of them. What happens to them on the ground is a matter then for those individuals. I do not have a remit to prosecute.

Joanna Cavan: I think it is important to distinguish as well whether it was wilful or reckless use. In these cases we were satisfied that they did not intentionally breach the legislation, it was just lack of knowledge and lack of training that led to these unfortunate errors, but it will be up to the local authority to decide. In one of those local authorities they ceased to acquire communications data until they were satisfied they had put robust systems in place to prevent recurrence of similar errors.

Q685 Mr Brown: Should you have a remit to prosecute?

Sir Paul Kennedy: In some respects I am half inclined to say yes, but on the whole I would prefer to say no, because the way in which we operate, for most of the time, is to try and encourage compliance and not to act as some kind of dragon who is there to try and notch up how many errors you have made. Yes, we want to count errors but we want to try and ensure that local authorities do it right. That is why, for example, we have been hugely supportive of NAFN because we know NAFN does it right. What we are more inclined to say is, “You got it wholly wrong, please use NAFN”. I think that is a more effective way, from the public point of view, of getting compliance than saying, “We will prosecute you”.

Mr Brown: If you uncovered something that you felt ought to be prosecuted, who would you ask to prosecute it?

Sir Paul Kennedy: It depends on the context. If it was within a police force we would probably go, in the first place, to the Chief Constable and say, “Here is the matter. What are you going to do about it?” In the last resort I can of course go to the Director of Public Prosecutions and say, “There it is”, but we have not had to do that so far.

Mr Brown: Thank you very much.

Q686 Dr Huppert: Sir Paul, your written evidence says, “It would be helpful if the record keeping requirements were extended to collect statistics in relation to the number of applications, the necessity purpose under which the data was acquired and the specific offence or crime under investigation. This would enable more meaningful conclusions to be drawn and would provide a further indication as to whether public authorities are using their powers appropriately.” If organisations are not keeping the statistics about application numbers, the purpose and the offence or crime, how do you verify that they are behaving proportionately?

Sir Paul Kennedy: The answer is they do keep the statistics but if they were required to keep them it would be much more accessible.

Dr Huppert: So they keep them in an inaccessible way. What are you saying? They either collect them or they do not, surely.
Sir Paul Kennedy: They all keep them differently, or not a lot of them keep them differently, and what we are trying to do is to say it would be a great help to us if they were required to keep them in a way that would be easily accessible so that we can present figures to you of applications. At present we cannot do so without getting co-operation from a whole lot of different people.

Dr Huppert: Your written evidence says that you want the requirements to be extended to collect statistics.

Sir Paul Kennedy: Yes.

Dr Huppert: Which is not quite the same as saying, “I want them in a format we can read”. Which one do you—

Sir Paul Kennedy: Both. We want them in a form that can be read too, yes.

Joanna Cavan: At the moment they would need to trawl their systems and there would be an element of manual counting, which obviously is not feasible when you are talking about thousands of requests. So, yes, they can find the information out for us and quite often we do put more specific requests when we go to inspect around certain types of data, certain date periods, certain statutory purposes, but depending on what system they are working on it can be quite time-consuming for them to do that, because the systems have been built around the requirements in the current code of practice. So if the requirements are updated and there is a new list of information that they must provide statistics for on an annual basis, then the systems will be able to be rewritten.

Dr Huppert: What you are saying is that we could have a system where of the 500,000 or so requests a year it would be possible for, say, this Committee to be told how many there were for which crime, how many for what sort of purpose and so forth, which we simply cannot do at the moment?

Joanna Cavan: Yes.

Q687 The Chairman: Would you be happy then with a schedule attached to the Bill setting out a standard format for reporting or something like that?

Joanna Cavan: I think it would normally be introduced through the code of practice.

Sir Paul Kennedy: In the Bill there would have to be a code of practice, so the opportunity is there for this particular suggestion.

The Chairman: It seems ironic we have a Bill that allows the automatic interception and collection of billions of bits of information but there is no method by which you can automatically get the information to publish.

Sir Paul Kennedy: I agree.

The Chairman: It would seem to me that what is sauce for the goose and so on.

Q688 Stephen Mosley: Some of the witnesses we have heard have suggested that individuals should be notified if their communications data had been obtained by an investigator under the RIPA powers—I guess there is an exception there if there is a criminal case that is ongoing or something—but do you have any views on that?

Sir Paul Kennedy: I do not favour it. Almost all the mistakes lead, for example, to your mobile telephone number being obtained and nothing happens, but an error has been made. For you then to be contacted to be told that your mobile telephone number was obtained by error does not seem to me to take anybody anywhere further forward. The vast majority—and I am
speculating now, I agree—of these inquiries arise out of a criminal investigation in some form or another.
It is also worth remembering, as one goes along, that we see—not a lot—from time to time investigations that have resulted in innocence being proved. What do you do about those? Somebody may have come into the frame and then the data investigation has shown they are not in the frame. I do not think they should have to be told that they were ever in the frame. If you look at what comes out of an error you very soon find that it is an error simply because nothing has come out of it and I do not think the individual would learn much by knowing, “I was the subject of an error”.

Q689 The Chairman: Sir Paul, I thank you very much for your patience—we are running a little bit late—but finally could I ask you about the filter? You said you may be slightly vague about what the filter will be at the moment but we have received evidence questioning whether the results of the filter will meet evidential standards given that no one entity could be in a position to say, “That is my data from Mr X going to Mr Y that travelled down our line only”. If we have deep packet inspection, which is picking up bits and pieces with regard to a BT line, a Vodafone line and a Facebook channel, they might not be able to say to the court, “We can vouch for the call sanctity of this package”. Have you a view on that? Are you aware of it?
Sir Paul Kennedy: Not a complete one because I think it would have to be tested in reality at the end of the day. But it is not unfamiliar to have evidence that comes from a source that is restricted. One can think of other examples of that where Parliament only permits you to do a certain thing, and that is what you obtain as a result. The fact that this falls in that category does not, of itself, mean that it will not be acceptable as evidence. It will come from a controlled source.
The Chairman: If I could clarify, I think what our witnesses were suggesting was that defence lawyers would be easily able to drive a coach and horses through it because hypothetically BT would say, “Well, here is what we have encrypted but we do not know if that is the Facebook bit or the Yahoo bit or someone else’s bit and we cannot vouch that that is accurate”.
Sir Paul Kennedy: I do not think that at this stage it is possible to give a firm answer to that, but it is not necessarily a no at all. Furthermore, in this field an awful lot of the information you are seeking is an order to forward an investigation. It may in the end never require to be used in evidence—and that is certainly true, for example, about the argument in relation to interceptors’ evidence. We get a lot of information that is very valuable and it is never used in evidence, so I do not think that that aspect of it is anything to be terribly worried about. We can deal with it when the time comes.
The Chairman: Mr Huppert on this point, because we are running rather late.

Q690 Dr Huppert: Presumably, as communications have become more complex, more and more of the data would be received through the filter, so if there are questions about the evidential nature it would mean that effectively you would be less and less likely to be able to use any of this communications data in a court.
Sir Paul Kennedy: It would have to be tested. I am just not prepared to say that it is inadmissible. I think it might be admissible.
The Chairman: Sir Paul and Joanna, thank you both very much. I am sorry we started late. We have overrun. That is testimony to the quality of the evidence you have given and the interest colleagues have in it. Thank you very much for coming. I wish you a happy retirement as from 31 December this year. Thank you very much.

Sir Paul Kennedy: Thank you very much. Thank you for listening so carefully and receiving us so courteously. I hope we have been of some help. If there is anything more we can contribute, we are very happy to do so.

The Chairman: Thank you very much. We will go straight on to our next witness and keep our fingers crossed for a vote, or keep our fingers crossed for no vote.
Examination of Witness

Christopher Graham, Information Commissioner

Q691 The Chairman: Mr Graham, thank you so much for coming, and profuse apologies that we are 30 minutes late. We were starting 15 minutes late because of a vote and we even then overran talking to Sir Paul. Thank you very much for coming. Just for the record, could you state who you are?

Christopher Graham: I am Christopher Graham. I am the Information Commissioner. I have been the Information Commissioner since June 2009. The Information Commissioner’s role is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for citizens. I have responsibility for enforcing the Freedom of Information Act and the environmental information regulations. For these purposes, the Data Protection Act and the privacy and electronic communications regulations are relevant.

The Chairman: Thank you very much. We are very grateful for your written evidence. You have nothing to add to that by way of introductory statement, I take it.

Christopher Graham: No.

Q692 Lord Faulks: Thank you very much indeed for your detailed written submission, Mr Graham, which we have all read. You make the point that it is for the Government to make their case effectively for this Bill but that some people might find their proposals difficult to justify, requiring the obligations that they do on providers. What category do you fall into?

Christopher Graham: You have quoted the second part of the statement. All I was seeking to point out was that there is a judgment to be made between the security community who say that we have to have this stuff and the civil liberties community, which says that this is a gross invasion of privacy and citizens’ rights. It is a judgment. To say that it is a judgment does not mean you have taken the judgment. That is for Parliament and for this Committee, having heard all the evidence.

For the Information Commissioner, the interesting questions are the practical ones: how this regime might work if Parliament decided it wanted to go ahead with the project. All I would say on the principle of the thing is to recall that six years ago my predecessor, Richard Thomas, sounded a warning that we were in danger of sleepwalking into a surveillance society. I think that had the very salutary effect of waking us all up. I do not think anyone would say that we are now sleepwalking. The evidence that you have already had, both written and in person, shows very strong arguments either way. The decision is for you and for your parliamentary colleagues to take.

Q693 Lord Faulks: Does that answer you have just given tie up very much with your very helpful recommendations about post-legislative scrutiny and the need for it to see how these possibly extended powers are progressing and possibly even to build in sunset clauses to the Bill?

Christopher Graham: That was a very strong recommendation that we made to the House of Commons Home Affairs Committee, which takes an interest in this sort of thing. We
commissioned a report on the state of surveillance in the UK, and we pointed out that it is all very well for Parliament, with the best of intentions to pass legislation. The thing is to see how it has worked in practice. That is what is happening with the Freedom of Information Act at the moment; the Justice Committee in the Commons has been conducting post-legislative scrutiny. This is jumping a few fences, is it not? It would be a good idea, if this Bill went forward, I will not say that a sunset clause be written in but certainly for a review to be envisaged, because on the face of it is a question of assessing the risks, and there are important data protection principles at stake. Whether the processing is fair and lawful is the first principle. The issues are very often around the seventh principle of security. There is a fifth principle about the retention of material for longer than is perhaps required. There is the principle of good practice of data minimisation. I think everyone would be concerned about the possible unauthorised access for retained material and perhaps the unlawful exploitation of the retained material, so it is really is for Parliament to keep a watch on these things. You can have commissioners charged with doing this and doing that, but this would not be one to legislate on and forget, I would suggest.

**Q694 Baroness Cohen of Pimlico:** What strikes me about this is that you have been given the duty, but I am not quite sure how you are going to do it. The only powers you are given under the draft Bill are those in Clause 22(5). Are these going to be adequate to enable you to protect the public? Is that what you think you are going to be required to do?

**Christopher Graham:** I am intrigued because, as you say, it is a duty but I do not see the powers. 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. I imagine that there would need to be some sort of inspection regime of the kind that Sir Paul has just been describing. I would like to think that if the safeguard was found to be credible, it would involve powers of audit of the communication service providers who have been designated under the Act, whoever they are.

I have to tell this Committee that I do not have those powers of non-consensual audit. I am asking for them in relation to local government and the health service, but I am not getting very far. I have those powers in relation to the privacy and electronic communications regulations for some communication service providers but only in relation to those regulations, so if the Home Office means that the Information Commissioner is really going to be able to reassure citizens that these communication service providers, whoever they are, are hanging on to the information satisfactorily and are getting rid of it finally and irreversibly after 12 months, I need the powers and the resources to do that, and if all there is is Clause 22 of Part 3 of the Bill, I am sorry but that does not do it.

**Baroness Cohen of Pimlico:** Thank you very much. I did not think it did either, so I shall be interested. We will have to ask the Home Office what they thought they meant. I loved Annexe A of your written evidence because the surveillance road map is just incredible. It is staggering as to who looks after what and who appeals to what. Do we see a need for a wholesale re-approach to all this, because it looks to me as though they have just handed you a few other clauses that put on you a duty to look after something else still but you do have
nothing to do it with. It is difficult if you ask who is responsible for the freedom of the citizen. If the answer is that you are, I am not sure you quite have the powers anywhere.

Christopher Graham: The road map was designed with the co-operation of my commissioner colleagues in different parts of the wood to explain how the terrain runs. As I say in the copy that you have had, it is very much a work in progress because things are moving all the time. For example, Mr Andrew Rennison has been confirmed as the Closed Circuit TV Commissioner, so there are some things to add there. The powers that be are in the process of appointing a Biometrics Commissioner, and so on and so on. It is a living document and was designed partly to make sure that there was very good communication between our various officers and that our staff understood how we should be working closely together. Also, now that it is in the public domain—and I do not think that a document like this has been designed before to inform the citizen of who can help—it identifies where there are gaps and where there are overlaps. It shows that some of us have powers to deal with complaints and others do not.

The Home Affairs Committee in the Commons that recently considered these things concluded that there ought to be either a single privacy commissioner or a sort of primus inter pares, and we would all be organised into one office. It sounds superficially attractive until you come to the Information Commissioner and you realise that my responsibility is both about privacy and about open government. I need to be able to take delicate judgments about when the data protection side needs to be paramount and when the freedom of information side needs to be paramount, so you could exclude me from some sort of single system. You do not need to have a single system and everyone in the same premises if we all understand what our various roles are. That was the aim behind the road map.

Q695 Dr Huppert: I will start with issues about how you keep security under review. One of the issues that many of us are concerned about is that data that is being kept may be inadvertently lost. Your office put out a statement today about a rather significant loss from Greater Manchester Police: the theft of a memory stick containing sensitive personal data that was not protected in any way and had the details of more than 1,000 people with links to serious crime investigations. I think you penalised them with a penalty of £150,000. Is this an issue to be concerned about with other collections of data?

Christopher Graham: That is the 26th civil monetary penalty we have had to impose. Greater Manchester Police got away with £120,000 because they got a 20% discount for early payment. We are a very reasonable authority. Nevertheless, it is undoubtedly true that the public service is not as good as it should be about keeping information secure. We have to work on that, which is one reason why I have asked for the power of audit, first of all of local government, which is particularly bad, and then of the health service, where the information is obviously very sensitive. Greater Manchester Police is not the first force we have had to issue a civil monetary penalty against. I remember the Lancashire constabulary quite recently had information about a very vulnerable missing teenager simply blowing down the street because the file was left in a squad car.

This is a worry, and it is a worry that the penalty for unlawful disclosure of information is so unconvincing. It is a fine-only regime, at the magistrates’ court at least. Section 55 of the Data Protection Act is not a very scary provision. There is work to do for Parliament, and I hope very much one of your conclusions may be to support the conclusions of the Home Affairs
Committee in the Commons or the Justice Committee in the Commons that we ought to get on and commence Sections 77 and 78 of the Criminal Justice and Immigration Act 2008, which have the potential for a stiffer penalty to be imposed. I am not sure that is going to get us very far in relation to what you are dealing with, because Sir Paul made the distinction between context and content, and communications here are supposed to be about context. So, yes, if my staff and I were asked to take on this role we would carry out our duties conscientiously, provided that we are given the resources—we would do it anyway, but we need the resources to do it, which is another story.

It is not quite the same thing as losing an unencrypted memory stick with the details of rather a lot of police informers.

Q696 Dr Huppert: Thank you, that is quite helpful on some of the security issues. You highlighted a number of concerns; I will come on to another one in a second. I ask this particularly because I note that the Conservative policy coming into the last election said, “Immediately submitting the Home Office’s plans for retention of and access to communications data to the Information Commissioner for pre-legislative scrutiny”. Did you have that opportunity?

Christopher Graham: When I came in, in 2009, this was a very live issue. I remember having a very fierce letter from the then Home Secretary before I had even been appointed saying that the interception modernisation programme, as I think it was then called, was an absolutely priority and that I must realise that we live in a world of terrorism and serious crime and must shape up generally. I said, “How very interesting, I look forward to discussing it with your officials”. The only discussions I have had with Home Office officials over three years have been about the theory. I have had a series of presentations where I have been shown a model of how communications capability is degrading, and the 75% figure is very familiar to me. My staff have then, because we were fairly sceptical in the evidence we put in in 2009 to the previous Government’s proposals, worked with the Home Office on doing a proper privacy impact assessment and the privacy impact assessment, which I think was published at the same time of the Bill. We certainly followed an ICO model of how these things should be done. At the end of the day, it comes down to that judgment, which is where you come in. 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.

We really do need now to get into the nitty-gritty of how this regime would work. It was very interesting that, of the 449 pages of evidence that were submitted to you in the first wave—I have not gone through the latest lot—there was only one estimate of the scale of the information that would be retained. Someone said that if you take 1% of all the internet material in the UK over a year, you get to 10 petabytes. I did not quite know what a petabyte was but technologists here will recognise that it is one hell of a lot of material. It is actually the same amount that Facebook identified in a prospectus for its recent initial public offering of all the audio and all the video that it retains. So we are talking about a billion customers worldwide of the most successful social network. That is the scale of what we are dealing with. If I am going to be asked to keep that under review to any purpose that a citizen would find reassuring, that is some task. I do not quite know how I would set about doing it because I do
not quite know, and I do not know whether I am going to be told, who the communication service providers are. Even when I know, I will need to have the resources to do the annual inspection that I suppose would be required, but then I also need to recruit the technologists to undertake the sort of spot checks that your constituents and citizens would find convincing. So I would need the powers and the resources to do that, and we would need to get into very detailed discussions with the Home Office to find out how it envisaged that this would work if the Bill proceeded.

Q697  Dr Huppert: I will very quickly pick up on one thing that you mentioned and that I was going to raise anyway: the list of service providers who are required to keep this data. According to your written evidence, the Home Office will not tell you on the grounds of national security who you are supposed to be checking up on. Is that right and is there any promise that it would change that in the new regime?

Christopher Graham: I only know what I know. You might say, “Well, you have not asked”, but I am sort of waiting to see how this process continues. It is not rocket science. The six largest ISPs in the UK account for 95% of the traffic, so I assume that British Telecom, Virgin Media, TalkTalk, Sky, O₂ and Orange will be candidates.

Dr Huppert: You would not know whether a small provider was or was not, and hence you would not be able to check whether or not they were complying.

Christopher Graham: If nobody tells me, I will not check, so that is no great reassurance. Also, I hope that I am not being overly sceptical, but I notice that the ambition is to increase the capability from the existing 75% to 85%, which leaves 15% still uncovered. Again, I do not think I am saying anything that is wildly controversial when I point out that if you are the international terrorist or the organised criminal who this system is designed for, you will presumably have the wit not to go with one of the big six. You will find a small provider, and you might even be able to afford the £5 a month to buy a virtual private network registered overseas. All your traffic will then be encrypted and you are home free.

I think the really scary people will have worked that out for themselves, so basically this is a system that, on the face of it, is looking for the incompetent criminal and the accidental anarchist.

Q698  Michael Ellis: Could I just make an observation, Mr Graham? If I may I will characterise what you seem to be saying at the moment as something of a power grab on your part, because you have made several complaints, it seems to me, that your powers are insufficient to do certain things. You want to increase the penalty powers, you want to increase your audit powers, you do not want to share powers with other commissioners as you do not think that would be right, your authority would not work as far as working with other commissioners is concerned, but it is the taxpayer who is penalised when police services are fined vast sums for losing memory sticks. Is it a fair characterisation that you are looking for more power from the Home Office and from Government?

Christopher Graham: I am looking for more powers to do the job that Parliament has given me to do. I merely make an observation about the safeguards and the limitations, which we called for when we put in our response to the 2009 consultation on the previous scheme. Apparently part of the reassurance is the Information Commissioner will be asked to keep something under review. All I am saying is that you want us to keep it under review. It is not a
power grab to say, “I will need to have the resources to do it”. Sir Paul just now said he had been assured that what ‘we need we will have’. I have received no such reassurance. The only resources I have on the data protection side are the £35 that data controllers pay for the Information Commissioner’s Office. The scale of the task is absolutely massive. I do not think it is a power grab to say, “Give us the tools and we will begin the job”.

Michael Ellis: The Interception of Communications Commissioner has received an assurance.

The Chairman: There is a Division in the Lords. We will need to suspend for a few minutes and we will reconvene as soon as enough Lords are back to make us quorate. Officially it is 15 minutes but we will try to be faster than that. Thank you.

The Committee suspended for 8 minutes for a Division in the House.

Q699 Lord Faulks: Further to the last question, I can probably anticipate your answer: you have obligations to keep a lot of things under review as a result of this draft Bill. The evidence we have so far had suggested the notices issued under Clause 1 will not be published. Have you received any assurance that notices will be available to you?

Christopher Graham: No, I have not. As I said, the work that will be necessary with the Home Office has not taken place yet. That is no criticism of the Home Office. I am sure that when you talk to Home Office witnesses at the end of this process, you may get more information than I have had up to now. I merely make the very simple point that if I do not know who has been the subject of an order, I am not going to be able to keep them under review.

As a postscript to Mr Ellis’s question before we were interrupted by the Lords’ Division Bell, I should just make clear that although the civil monetary penalties that I have the power to levy in respect of serious breaches of the data protection principle are up to £500,000, that money does not stay with the Information Commissioner but goes to the Consolidated Fund. So I do have this resources problem, not like my Spanish colleague, who raises the money for his office by fining people. Nor should it be like that. Just because £150,000—or £120,000, as it turned out—has been taken from the Greater Manchester Police, that does not help me any.

Q700 David Wright: You are also required to keep under review, Mr Graham, the destruction of data. I have read your submission notes. It is clearly important for the public to know that data is being destroyed appropriately. What is your reading of the content of the Bill, and how are you going to potentially achieve that review? Having read your evidence, I envisaged groups of people potentially sitting in yards outside office buildings putting sledgehammers through material in order to physically destroy data that is held. What is your view on this?

Christopher Graham: Again, it is more likely to be the very effective overwriting of information that is held wherever it is held. 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. That clearly is quite unacceptable, and we have to have a credible regime that can stop that happening.

**David Wright:** Other witnesses also have doubts about the practicality of destroying evidence so that it can never be retrieved, and one suggested that it would be more appropriate to repeat the requirement of the Data Retention (EC Directive) Regulations 2009, which is to, “Delete the data in such a way as to make access to the data impossible”. Reflecting what is possible today, would that be an improvement to the draft Bill?

**Christopher Graham:** I am not sure that it makes a great difference to mess around with the definition. You might just create problems in another part of the wood. The vital thing for this Committee to satisfy itself about, when you have heard from the Home Office, is how you can be sure that whoever is asked to carry out this inspection, whether it is the Information Commissioner or one of the other arrays of commissioners, is able to do the job in practice rather than just in theory.

**David Wright:** But your submission to us did say it is not clear how the requirement to destroy data relates to the way in which operators achieve the deletion of existing records in practice. Basically what you are saying is that the Bill as currently drafted does not clearly indicate what “destroy data” is. You have given us a comment today that you think it is potentially the overwriting of material. Would it not be better if this Bill specified exactly what “destroy” meant?

**Christopher Graham:** It is possible. My major concern is to understand how the supervision task—this is my perspective—is to be carried out with any credibility.

**Q701 Baroness Cohen of Pimlico:** What you are telling us is that you have not had the conversations with the Home Office on how you are to do all this, which you would expect to have and indeed that you have to have. Is it a fair question to ask whether you have made any calculations inside your organisation on the extra resources and extra staff needed to enable you to do any of this? We are thinking with one part of our minds about the cost of doing all of this, and the Home Office has provided us with an estimate, but I am not sure that it was thinking about the Information Commissioner. I may be doing it an injustice, but I am not sure that they were.

**Christopher Graham:** I hope the Home Office does not think this is something that I can do just from my own resources. It is the downside of the Information Commissioner being quite a high profile role at the moment and lots of departments of state having ideas such as, “It would be a jolly good idea to get the Information Commissioner to do this, that and the other”. In some ways it is good to be popular. On the other hand I have, as the chief executive, to keep my feet on the ground and say, “Excuse me, who is paying for all this?”, because I only have the resources that I have and we have the usual Gladstonian rules about not using freedom of information money on data protection or vice versa. I do not think I would be able to use either of those sources of revenue on this task, which is over and above the usual run of data protection work. I would be looking to the Home Office for grant in aid, and if it has not done its sums it better had. It simply cannot be a credible reassurance if it is not an activity by the Information Commissioner’s Office that is sufficiently well resourced, both with people and with funds, in order to do the job. It just does not deliver.

**Baroness Cohen of Pimlico:** Have you made any calculations of the kind of number of extra people you would need?
Christopher Graham: This is a chicken and an egg situation, because until I know the scale of what I am being asked to do I cannot do the sums. I simply flagged up to you in my written evidence, and again now, that here is an issue that we need to pursue. This is a draft Bill. If it proceeds, we need to have those conversations, but obviously organisations such as mine are planning all the time and it would be good to know.

Q702 Lord Strasburger: I have a quick question on destruction. When you are reviewing the destruction of data, how confident can you be that all copies of that data have been destroyed on the basis that there are multiple copies for back-up purposes and so on?

Christopher Graham: We have learnt from bitter experience in other cases that sometimes the things that we have been assured have been destroyed appear in caches here and there later on, so it is certainly a challenge. One certainly would be looking for a regime based on audit assurances and then some without-notice inspection. Again, it would be helpful to know the amount of retained material and therefore the scale of the audit task that I have to undertake. At the moment, all we have is a proposition but no detail.

Q703 The Chairman: On destruction, it would seem that one gap which the Home Office is concerned about is the social media providers: the Facebooks, Yahoos, Googles of this world. If they decide to co-operate with the Home Office and create the systems to collect and store their 10 petabytes of information on their servers in California, how are you going to inspect Mr Google and Facebook and so on and make sure they have destroyed it?

Christopher Graham: In that they are not within the jurisdiction?

The Chairman: They will be storing information on British subjects in their servers in California.

Christopher Graham: Or wherever the information is stored. Google is quite a good example, because at the end of the recent Google street view affair we persuaded Google Inc to volunteer for a good practice audit by the ICO. It did not have to do it—well, practically it did because it was in so much trouble, but I could not make it do it. We certainly found with Google that we were dealing with a professional outfit. It understands the business that we are in and we are talking to grown-ups. My colleagues in the Irish Republic have the same sort of grown-up relationship with Facebook, so it can be done. No doubt the social network sites that receive these orders from the Home Office will behave appropriately.

The interesting thing is what happens about the 5% of traffic that is going through the small providers that nobody knows about it. These can develop very, very quickly. I saw a graph the other day of the impact of the Angry Birds game on iPhones. Suddenly something becomes very fashionable very quickly in the same way that some things that were incredibly fashionable then just tank. But over a very short period an internet service provider can grow from nothing, and I suggest that your organised crime and your terrorist groups are going to be using those guys. How quickly are they going to be designated by the Home Office? How quickly can we find out what is going on there? It is a very challenging environment and a very challenging task that we are being asked to undertake.

Q704 Lord Strasburger: Can we turn to judicial approval for access? If and when local authorities have access to data retained under the Bill, this will be subject to judicial approval. Some of our witnesses have suggested that access to data by all public authorities, including
your own, and the security and law enforcement services should be subject to judicial review. What is your view?

Christopher Graham: I have to declare an interest. As you have just pointed out the Information Commission’s Office itself makes use of the communications data in order to enforce the privacy and electronic communications regulations and the Data Protection Act, for example. That is a very important part of the weaponry that we have at our disposal to deal with the scourge of spam texts, unsolicited emails, and worse: the unlawful access to private information from databases in breach of Section 55 of the Data Protection Act.

You may say this is rather self-serving. I would say that the purpose for which the Information Commissioner might require that is always going to be slap bang in the middle of enforcing the duties that Parliament has given us to deal with. It is not going to be controversial. Sir Paul’s inspectors go round the ICO and check that we are compliant with the Regulation of Investigatory Powers Act. I think that is a system that works. I was quite struck by the point Sir Paul made to you when he talked about the effect that a warrant regime would have on speed of access and the sorting of information that is needed to deal with unlawful activities. It is only an opinion, but I am not particularly persuaded by that.

Q705 Stephen Mosley: I was going to ask you the same question as I asked in the previous session. We have had suggestions that individuals should be notified if a request is made about them. Do you have any thoughts on that?

Christopher Graham: Again, I do not think it is something for the Information Commissioner to give a view on, but if you ask me I will give you a private view. I think the only circumstances in which communications data would be lawfully requested—and if it was not lawful it would be caught by the inspection regime—will be because there would be something to be investigated. If we are saying that individuals then have to be notified, that could obviously be a problem in the course of an investigation. If the Home Office says that this is about serious crime and terrorism, that would not be a good idea. If people had been eliminated from inquiries, what is the point in telling them that they were in the frame but they are not now? From a citizen’s point of view, I would not go down that route.

Q706 Stephen Mosley: Under the Data Protection Act, individuals can make requests to companies to see the data that they hold about them. The Home Secretary is able under Clause 1 to specify what data those companies hold on an individual. If they put in a Data Protection Act request, they would be able to see that information, so surely within a very short period of time people put in requests under the Data Protection Act, find out what data is being held, and are quickly able to work out which communication service providers are holding the data and what data they are holding. Do you think that the secrecy about the data retention notices and Clause 1 will soon be circumvented by people putting in data protection requests?

Christopher Graham: Concerned consumers and citizens would shop elsewhere if this sort of thing concerned them. Yes, they do have the right of subject access under the Data Protection Act. I do not think it is rocket science to work out if you are a customer of British Telecom, Virgin Media, TalkTalk, Sky, O2, or Orange that you are going to be on the list. You do not need to put in a subject access request to work that one out.
As I say, I trust that the Home Office is at least going to inform the Information Commissioner which of these communications service providers have been designated, or I cannot do the checking.

**Stephen Mosley:** You say there are a number of providers that are obvious, and there are, but you surely must be able to imagine a situation where interested parties put a request to every CSP they can think of, find out what data they are holding and therefore know which ones are affected by Clause 1?

**Christopher Graham:** I cannot fault the logic of your argument. One can imagine that the volume of subject access requests that communication service providers would face would be unsupportable, quite honestly, if that is how constituents wanted to play it. The Home Office will surely consider the wisdom, or the unwisdom, of keeping the information about designated authorities to itself because it may, as you point out, be information that is outed anyway.

**Q707 Stephen Mosley:** At the moment, though, Clause 1 does say that it is in effect secret. Because it can be circumvented in the manner that we have just described, do you think that the Home Office should just be up front and open about who it is putting Clause 1 requests into and what data to ask them to hold because it would be found out anyway?

**Christopher Graham:** That is one for the Home Office. I suppose it might say that the whole business of communications capability is a consideration of the behaviour of criminal and terrorist elements and that you do not want them to know too much, but I am not sure that what is apparently envisaged in that part of the Bill is doable.

**Q708 Lord Strasburger:** On the separation of data and content, some of our witnesses have commented on the difficulty or even the impossibility of separating communications data from content, particularly in an encrypted situation but not only an encrypted situation. What is your view?

**Christopher Graham:** To many people, communications data is content. It is very informative. You do not have to delve into the substance of a message to draw conclusions about the sort of communications that people have, which is why the authorities might be interested in it. But then one can understand why there are civil liberties issues and why critics of these proposals are saying, “I do not want the state, in effect, to have access to the communications I am having with my doctor, with that mental health helpline”, or whatever it might be. I am not sure that you can make the contrast between content and context, even though it is reassuring to know that this is about establishing who was talking to whom, where and when rather than about the substance of what they were talking about.

**Lord Strasburger:** I think we understand that the data can in a lot of cases give a very good clue as to content or pseudo content, but this question is driving at how easy it is to separate that data from the true content of the communication, and encryption is a particular area of difficulty, but we have been told by other witnesses that there are also other areas of difficulty in separating the content and the data.

**Christopher Graham:** Yes. I do not claim to be a technologist. Encryption, which of course is something that, while wearing another hat, I very strongly advise would frustrate the purpose of this Bill to track the communications from someone who is of interest to the police with somebody else. It is not difficult to see that encryption is a good idea for security reasons. If
only that memory stick that the Greater Manchester Police detective had stolen from his house had been encrypted we would not have the problem that we have. So the Information Commissioner spends most of his time going around urging everyone to encrypt everything, and of course good businesses do that. Individuals can do it too for £5 a month, so, surprise surprise, they will. That then frustrates the whole purpose of this Bill.

**The Chairman:** Slightly hypothetically—and I do not want to put you on the spot—could you therefore envisage circumstances in which, if you do not get the resources you feel you need, you do not have the access you feel you want, and you are not given the information about the CSPs that are on the Home Office list, the Information Commissioner is going to urge the British public, “Encrypt everything, it is the only way we can protect your privacy”? That is a slight exaggeration, but I am putting it that way for effect.

**Christopher Graham:** We pretty much do that anyway. We certainly do it with companies, and I would not do anything so incendiary as to say, “Encrypt everything so you can frustrate the Home Office”. All I am saying is that there is a lot of encryption going on, and there will be more encryption. It is a fact of life.

There is another aspect to this Bill. I hope that the Home Office could convince me otherwise, but there is something a bit Canute-like about this whole thing in that we are raging against the onward march of the modern world. The 75% figure arises because of the spread of communication through the internet. It is just a fact of life. You can get from 75% to 85% if, if, if—or can you? But the terrorists and criminals you are interested in will respond, the technology is there to respond, so, at the risk of mixing my metaphors, it could be a bit of a chimera. There is an objective which the security services tell us is absolutely paramount and that we must have, but is it achievable?

**Q709 Lord Faulks:** You described some current abuses. The Bill envisages further data being retained. Do you have any comments about the possibility of abuses if this Bill becomes law?

**Christopher Graham:** I am very concerned anyway about the security of information in large databases, whether they are in the public sector or the private sector. I do not think that as a society we take this nearly seriously enough. The fact is that if you are taken to the magistrates’ court for the unlawful disclosure of information under the Data Protection Act, or for dealing with rogue employees or people who simply see a way of making a fast buck and selling information—possibly to journalists but not normally to journalists, actually, usually to claims management companies—or even in pursuing private vendettas or family disputes, the response from the court is pitiful. The going rate is a fine of £120; it is a fine-only regime. It has to take into account your ability to pay, and at the moment the going rate is £120. If you are a private investigator and you are in the information business it is just a business expense and you go on your merry way.

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. Of course what it does is to access all those potential deterrent penalties, community penalties, and so on, which the magistrates’ court simply cannot do at the moment because all you can do is say, “We are going to fine you and, oh dear, you do not have any money, so it is £120”. We have to take this more seriously, particularly if we want to get all the benefits that the internet and online can offer for the effective and efficient delivery of public services. We have to get the confidence of citizens
behind sharing data, for example, provided that is done sensibly and legally. You will not get that confidence if all people read about in the newspapers is that this local authority lost that piece of information, or this police force lost that piece of information. We will not get the confidence unless we have an effective deterrent regime in place, and we do not have that now.

**Lord Faulks:** You have given evidence along these lines in the context of the Leveson inquiry, have you not?

**Christopher Graham:** I have. I have to say that one of the despairing things about my otherwise fascinating job is that I have been saying the same thing for over three years and I am beginning to think it must be me, because parliamentary committees have bought the argument and reported and absolutely nothing happened. I hope I have convinced Lord Justice Leveson, but we will have to see.

**Lord Faulks:** You specifically refer to the police forces routinely accessing individuals’ mobile phones on arrest. They gain access to information held on the phone even though the people may not be suspected of any wrongdoing. Do you understand that to be a lawful use of that opportunity?

**Christopher Graham:** My office is currently investigating the lawfulness of these cases that have come our way and what steps can be taken to prevent it. When we have reached a conclusion I would be very happy to update the Committee, but there seems to be a distinction between a policeman on arrest looking to see who is on your mobile phone, who your associates are, who you text, and looking at the content of your messages, your inbox, the names and so on. I am concerned about this but I do not know what the answer is. As soon as we have a conclusion, I would be very happy to update the Committee.

**Q710 Mr Brown:** Can you tell us something about the mutual legal assistance process? For example, do you have any direct supervisory role over it, and do you think it is effective?

**Christopher Graham:** We do not oversee applications for mutual legal assistance involving communications data. We have no involvement on compliance issues on which to base any view about the current process, and I understand that the UK-relevant central authority is the Home Office, so I cannot help you, I am afraid.

**Mr Brown:** But should it be you or is it best that it be left with the Home Office?

**Christopher Graham:** If Mr Ellis was here he would find this hard to believe, but I am not looking for work.

**Mr Brown:** He is not here, tell us what you really—

**Christopher Graham:** I am very happy to leave that to the Home Office, of course. The Information Commissioner’s Office is involved with a lot of liaison with other data protection authorities across the European Union and elsewhere, and we are active in our work in the Article 29 working party on the revision of the data protection regulation. I am off to the international conference at the end of the week to liaise with the Americans, the Australians, the New Zealanders and practically everybody else, because this is a global business that we are in and it is no good having a regime that works just in the UK, particularly if you need to retrieve fugitives from Bordeaux, for example.

**Mr Brown:** Do you think these arrangements work well or have you just not formed a view? If you are a public authority that used the powers that they have but rarely, is this a reasonable route for them to go?
Christopher Graham: I should not stray into a territory I do not know an awful lot about. It has not come across my desk. The mutual legal assistance scheme has not come across my desk.

Q711 The Chairman: Finally, or penultimately, commissioner, you have just said that you are involved in international discussions with your international colleagues. If this Bill were to go ahead, would the UK be in a unique position with these proposals—unique in the technological side and unique in the level of data gathering and intrusion?

Christopher Graham: I know that the data retention directive has run into a lot of trouble in different jurisdictions in the courts, and that was just the previous data protection directive, so I do not know how this would fly. We are assured by the Home Office that it is compliant with the Human Rights Act. I am sure there will be lots of people queuing up to challenge that, but that would have to be seen.

The interesting thing is how this whole area plays out at the moment, because we have very complex negotiations on the regime that will replace the current Data Protection Act, which follows on from the data protection directive, which is in the process of being reviewed. It looks as though we are going to get a regulation instead of a directive: in other words, something will just apply directly, as you know, without the need for transposing everything except police and justice, which is or is not going to be subject to a separate, new directive. I wish it was possible to have a clear set of rules that just applied to all data protection activities in whichever sector. I cannot believe that it is a good idea for police forces to have to conduct some of their work under the new proposed regulation and some of their work under the new directive, if there is a directive, but that is probably an argument for another place.

The Chairman: But that directive might have less stringent requirements than the general regulation, which could result in some member states lowering standards. Would the UK be one of those states with lower standards?

Christopher Graham: There are differences of opinion around the table in the Article 29 working party on where the regulation that applies to everything apart from police and justice is unacceptable because it set standards that are too high and too rigorous or that it is unacceptable because it set standards that are less than the standards that are enjoyed in many member states.

In the case of policing, it is important to make clear that the proposed directive would not, as I understand it, affect domestic policing. It would affect only the transfer of information across the borders and so on.

The Chairman: Thank you very much. Any other final questions?

Q712 Lord Strasburger: Just one question. Coming back to encryption and CSPs that are not within the system, is it possible, in your mind, that the implementation of this Bill could have the opposite effect to the one that is intended and that when the bad guys have moved to encrypt their information and to avoid the ISPs that are being monitored, the public authorities end up with access to less data than when they started?

Christopher Graham: I suppose that that is a hypothetical case that you are advancing, and I hope that nothing I have said this afternoon has made that more likely. On the other hand, it is just in the nature of things. That is the way in which things will go. The questions then arise: what resources are going into this; how much are those communications service providers
who are identified going to have to be paid to do this task; how much is the Information Commissioner going to have to be paid; how much is Sir Paul Kennedy going to have to be paid; what is the total cost of doing something that may be of marginal benefit at the end of the day? Those are questions that I am very glad to leave to you people to decide.

Q713 The Chairman: Sorry for prolonging the session but I have one final point. Your discussions have provoked me. As parliamentarians we always want to pass a law that will last for a long time. As Ministers we know you get one shot at a bit of legislation every five or 10 years. There is a hope here that if the Bill seems to be drafted to a certain width, it will stand the test of time, but is that—and I do not want to put words in your mouth—a rather naive view of legislators? When the technology is moving so rapidly, is it possible for us as parliamentarians to pass a RIPA mark 2 2012, which will last to 2020 without being fundamentally wrong?

Christopher Graham: I think that a confident Parliament would nevertheless include a commitment to post-legislative scrutiny after five years or so, not just because the technology is changing but because you want to see how it works out in practice. I think that is a good thing to do, and it is one of the assurances that Parliament can give to a concerned citizenry when we are dealing with these surveillance matters that we will look and see how it works out in practice as well as in theory.

So I do not think you convince anyone if you say, “The laws that we pass are so wonderful, so we will not look at them for 20 years”. I think Parliament will say, “We have gone through a thorough pre-legislative scrutiny. We have heard all the voices. This is what we think. This is what gets passed and we check how it is going in five years”.

The Chairman: Thank you very much, Commissioner. It has been a long session. We all thank you once again for your excellent written information. The surveillance road map is particularly interesting. I think we all learned from it, particularly that we are going to have new commissioners for cameras and surveillance and other things, which some of us were not quite aware of. Thank you very much for the written evidence and for your participation today. It has been a long but very worth-while session, and keep up the good work. We cannot make promises on resources, with or without Mr Ellis here, but good luck on what you do.
WEDNESDAY 17 OCTOBER 2012

Members present

Lord Blencathra (Chairman)
Lord Armstrong of Ilminster
Lord Faulks
Lord Strasburger
Mr Nicholas Brown
Michael Ellis
Dr Julian Huppert
Stephen Mosley
Craig Whittaker
David Wright

Demos [Jamie Bartlett] (QQ 714-734)

Examination of Witness

Jamie Bartlett, Demos

Q714 The Chairman: Welcome, Mr Bartlett. Thank you very much for agreeing to start early. We are expecting votes today, so we may as well kick off when witnesses are ready to go. We have a range of questions to ask you, but I begin just for the record by asking you to identify yourself and say who you are.

Jamie Bartlett: My name is Jamie Bartlett and I am the director of the Centre for the Analysis of Social Media at the think tank Demos.

The Chairman: Thank you.

Q715 Michael Ellis: The Committee understands that your primary research areas—and please correct me if I am wrong—are terrorism, radicalisation, extremism, conspiracy theories, of which there is no shortage on the social media or the internet, and integration. Is that right?

Jamie Bartlett: That is correct, although more recently I have turned my attention to surveillance technology and its implication for security.

Michael Ellis: So, areas not unrelated to the interests of this Committee and this scrutiny. Do you or your organisation, Demos, have any views on the adequacy of RIPA as it currently stands for the work of the law enforcement agencies?

Jamie Bartlett: Yes, we do. RIPA was passed into law a decade ago, at a time when the majority of requests for information through it were for telecommunications, bugs in houses, phone taps and the like. Particularly over the past five to 10 years, but increasingly over the past three years, an increasing amount of communication takes place in neither an obviously private nor obviously public sphere, through social media. The problem is that social media offer a lot of potential very valuable intelligence and information for law enforcement and other arms of government as well, but how it is collected—how the harms to people’s privacy are measured, managed and regulated—simply has not really been addressed yet under RIPA, for obvious reasons. The problem is two-fold; it means that intelligence agencies and security
services more generally do not really know the extent to which they can under RIPA access information and intelligence that might be of use to them through these new mediums of communication. Secondly, it means that without that regulation, which reassures the public on how social media data are collected and analysed—that it is done on a legal footing—there are rife conspiracy theories, as you say, about how the arms of the state collect this information without our consent or knowledge.

The Chairman: I need to stop you there because there is a Division in the Commons. We will reconvene as soon as a majority of members are back.

The Committee suspended for a Division in the House of Commons.

The Chairman: Mr Bartlett, can you remember where you left off?

Jamie Bartlett: I was simply stressing that new forms of communication, in particular social media, have meant that RIPA in many ways does not cover public reassurance adequately and does not create an environment in which agencies can feel confident.

Q716 Michael Ellis: So from both angles, from that of the security and intelligence agencies, and from that of those motivated to consider the civil liberties aspect of these matters—or the parameters of the authorities’ actions in collating communications data, there is a need for a new legislative measure. Would you agree?

Jamie Bartlett: I absolutely would agree. In fact, the draft Bill does not cover anywhere near enough the new requirements that law enforcement agencies need in this new environment.

Michael Ellis: It is in the interests of all sides that there be set out proper parameters within which the authorities can act and which those who wish to monitor the authorities know exist.

Jamie Bartlett: Precisely, but the problem here is how you maintain the association between not two but three different classes of public good. So there is the maintenance of national security and public order and citizens’ right to law, liberty and privacy, but also the economic and social well-being of the nation, which is vital when considering how you would go about intruding on people’s privacy in this space. The problem of course is how you do that in a period when people’s views on privacy in this new area are in no way settled; they differ vastly across different segments of the public. Necessarily, security threats are changing and are not always well known, and the technology required to do this is often unclear in how it would work and the ramifications that it would have not just next year but in 10 years’ time. If RIPA was out of date five years after it was passed, the speed of change, with the capabilities of monitoring technology now, is such that any Bill passed now is likely to be required to be reviewed within two or three years. This is the great difficulty, and why I think that a much broader conversation about the nature of intelligence work on the internet more generally is required beyond just communications data.

Q717 Michael Ellis: For the moment, with the Bill that is the subject of this scrutiny Committee, from what you have said it is clear that the current law is inadequate and that it is likely to be more and more inadequate. Therefore there needs to be a new measure. You have indicated that you do not think that this draft Bill, which I am presuming you have studied, does not go far enough? Do you think that it would nevertheless better equip the security and intelligence services for the essential work that they have to do?
Jamie Bartlett: I have no reason to doubt when the Home Secretary wants to put this measure into place that it would facilitate law enforcement agencies to do their job. Most of the people I speak to about this would probably rather they did not have to introduce such an expensive and obviously controversial measure. The problem is that RIPA and the other regulations are there also to reassure the public. In that sense, probably because of a combination of good advocacy work and poor journalism, the way in which this Bill has been reported does not command public understanding or agreement in any meaningful way. This is really important because it has been described consistently as a “snooper’s charter”, but a snooper’s charter is about being able to do phishing expeditions that are widely possible now, outside RIPA, through going on to open-source social media sites and monitoring huge volumes of data about people. That is the perception that people have about what this Bill is about, and that is not what it is about, which is why I think it needs to be widened, so that that type of monitoring is regulated and brought under some kind of legal footing.

Michael Ellis: So it is actually diametrically opposite from those who call it a snooper’s charter, in your view, because the Bill would help to regulate where at this moment there is no regulation.

Jamie Bartlett: In some senses, yes, although there is a huge area that is not regulated in view under this Bill.

Q718 Michael Ellis: Can I look with you at the present law as it stands, and a couple of issues with it? The position of Her Majesty’s Government is that the present law does not require communications service providers to generate or retain communications data for which they have no need already. At the moment, they may have need for certain bits of data, usually for billing purposes, so they can bill people the right amount of money. But it does not require them to collate that data, or retain it, and it does not apply to providers based overseas. Do those issues need to be addressed and is it necessary for those issues to be addressed to allow the security and intelligence services and law enforcement agencies generally to perform their functions properly?

Jamie Bartlett: Part of the problem is that there has not been to my mind enough evidence to demonstrate the necessity of this, particularly through case studies and examples that allow the members of the public to understand the relative trade-offs in this Bill. I believe that it probably is necessary. It is worth mentioning, although I do not want to go into this, because other evidence that you receive will be far more accurate and knowledgeable than I can provide on this, that many major organisations already keep huge amounts of information on us. It may not be in exactly the way that security services want it, but a lot is available, because data are considered to be the raw material of the 21st century.

Michael Ellis: We have heard about supermarkets.

Jamie Bartlett: Of course, and Facebook has hundreds of thousands of pieces of information on most of its users. But on the second point and the international jurisdiction—

The Chairman: I am sorry, but we have another vote in the Commons.

The Committee suspended for a Division in the House of Commons.

The Chairman: We are back in session. Mr Bartlett, you were answering a question from Mr Ellis.
Jamie Bartlett: Yes, I was just going to say that I cannot answer this question particularly well and I do not want just to gas off when I do not have special knowledge, but the international point is a much broader one than you are probably going to be able to answer this Bill. Who has jurisdiction over the internet is, of course, far broader an issue.

Q719 Michael Ellis: You have already answered it in many ways, in that you have indicated in your initial response that you think that there is a gap in the law at the moment. I do not want to mis-characterise you, so please correct me if I am wrong. You think that that gap needs to be addressed both in the interests of law enforcement but also in the interests of those seeking to oversee what law enforcement does.

Jamie Bartlett: That is absolutely correct. Our national security strategy says that security and intelligence work is predicated on public consent and understanding. It is absolutely critical that we understand and give some kind of consent, ultimately expressed through Parliament, to the measures that are taken to keep us safe. That is why there needs to be an extension of surveillance and interception technology.

Michael Ellis: And if anything, you think that this Bill may not go far enough.

Jamie Bartlett: Correct.

Q720 The Chairman: Could I pick you up on that point, because I am slightly confused? You have just confirmed that you would like to see the Bill go further and be wider, but earlier in your evidence you said that part of the public concern was that the Bill seemed to be far too wide. Can you clarify that for me?

Jamie Bartlett: Yes, of course. In my view—and perhaps it is a little controversial—the Bill is an extension of existing powers. We have regulated surveillance and interception in this country, of course. As it stands, some of the data that some companies collect are not available to law enforcement agencies across the board. This is an attempt to make sure that that information is available. For example, putting a bug into somebody's personal living space would be far more intrusive, and we regulate that. But the problem is that although this is an extension of existing powers it is widely understood to be a complete and radical shake-up of how the intelligence and security apparatus work, essentially allowing the Government to snoop on everybody's e-mails, social media presence, web browser history and everything else that they do online. That is how the public in general, because of how it has been presented, believe this law to be about. It is a good opportunity to reassure the public about the broader way in which intelligence is collected from social media. The reason why it is an opportunity is because that is how it is being understood, which is inaccurate.

The Chairman: So on one hand you are saying that, yes, the security services need these additional powers, but we should therefore put more regulations in the Bill controlling surveillance as well as stronger governance measures. Is that what you are saying?

Jamie Bartlett: Correct.

Q721 Lord Strasburger: I take your point about the proposed Bill being an extension of existing powers. Can I perhaps explain your puzzlement at the public reaction in this way? Is
it possible that the public are ignorant and unaware at the extent of intrusion that is taking place right now under RIPA? The introduction of this Bill has woken them up to what is going on already.

**Jamie Bartlett:** First, I and the advocacy groups that work on behalf of privacy, in particular, cannot really claim to speak for the public. I am not actually sure what the public think about this Bill; it is not necessarily what journalists have reported about it or what advocacy groups say about it, me included. There is a distinct lack of information about what the public think about surveillance technology in general. It is possible that the furore around this has woken the public up to surveillance technology, although I do not happen to think that what is being proposed here is anywhere near as intrusive as some of the things that commercial companies already do on a daily basis, so I would be rather surprised if that were the case. Instead, the reports that I have read about it have tended to say that the Bill gives unfettered access for the Government to snoop on your behaviour online, which I would consider quite inaccurate. It is regulated; it might not be perfect, and there are changes that I would suggest, but if that is how it is being widely reported, I think that it is a mis-characterisation.

**Q722 Lord Armstrong of Ilminster:** Following on from that, my impression is that the Home Office thinks that this Bill is as wide as it is to provide cover for a long time for what it needs and wants to do. That is one reason why the powers are very general. I think that I hear you say that if that is its object it will not succeed. Is that right?

**Jamie Bartlett:** What I am trying to stress is that there is a lot more regulating and putting on a legal footing how intelligence and security services access information that is online but that is not included in this Bill. Let me give you an example of directed surveillance: in other words, a police officer following an individual and collecting information about him on a public highway. That requires some kind of authorisation; it is quite low, but it is required. To do the equivalent on the internet, to collect information about any of you or about me or any suspect, and to gather a profile on that person, requires no authorisation whatever. It can just be done—any of us could do it. To me that suggests that there is a discrepancy, which leaves agencies unsure about the extent to which they can go and access these potentially very valuable sources of information legally and on a sound footing, for reputation as well as legally. That is where this Bill needs to go, to broaden out.

**Q723 Mr Brown:** You said earlier that you could suggest some amendments that would add to the public protection and safeguard against misuse by operatives. Could you spell that out for us?

**Jamie Bartlett:** Yes. The first thing is the critical point, which is to make sure that it is based on some form of public consent. The process by which the Bill has so far proceeded, given its importance, has not been sufficient to do that. Clarity over certain issues, to allow an open debate in the House about what is to be done about Schedule 1, the nature of the technology used, international agreements for data-sharing and exactly what is going to be collected, is absolutely critical to allow us to have a reasonable discussion about the various trade-offs that the Bill will inevitably entail. I mentioned already the legal footing for social media intelligence collection, which is not covered. On the Bill in particular, the first thing is that the whole of the intelligence apparatus in respect of RIPA and other regulations is built on a kind of sliding scale, whereby the greater the degree of intrusion, the more oversight is required.
and the fewer agencies are able to do it. In this Bill, the distinction made between communications and content data is obviously blurred in a way that it was not under telecommunications. The existence of a telephone call between two individuals is utterly distinct and easy to collect differently from the nature of what is being said in that conversation. Traffic, use data and subscriber data rather blur that boundary. I would suggest that to maintain that association and that scale between the degree of intrusion and the limits on who can do it and in what circumstances, you might want to look at making a distinction between use data and traffic data, for example. This is technologically potentially difficult, but I see that there is a true difference in the type of websites that you visit and the browser history in use data; that is more of an intrusion of privacy than the existence of a communication between two people. For example, there is a way in which you can maintain that sliding scale, by making a distinction so that it is not as clear-cut as content versus CD information. That being the case, I would then recommend that judicial warrants might be applied—something that is often discussed, particularly in the case of use data. One of the biggest concerns is that, for all the possible arguments over whether it is more effective to have an inter-agency sign-off versus a judicial warrant, the problem is that, as far as I can tell, the public would be more confident with some obviously independent system of judicial oversight. With use data, in particular, that could be very significant.

The Chairman: Thank you very much. If you have ideas or a paper on a sliding scale or the difference between use and content, it would be very helpful to have it, because I do not think that it was in your Data Dialogue report.

Jamie Bartlett: No, it was not.

The Chairman: We would all find that very helpful.

Q724 Lord Armstrong of Ilminster: At the front of The Data Dialogue, you say: “The public must be at the heart of any new settlement on data sharing”. I wonder whether you could explain that, as it is a very general statement.

Jamie Bartlett: I will be quite brief on this. This was a paper on commercial use of personal information, by commercial companies. The survey that we conducted of 5,000 members of the public showed an increasing concern about how personal information and behavioural data were being accessed, used and shared and for what purposes. In general, members of the public that we surveyed for this did not see the benefits to them of sharing information. They had huge concerns about how it could be misused. Our argument was that commercial companies need to recognise that there is a commercial dividend to taking issues about personal information seriously, which means being open about how you go about collecting people’s information, how you are going to use it, what the public gets in exchange for sharing their information, how you are going to store it and how you make sure that it is looked after carefully. That is true, of course, for public agencies as well. All the surveys show that as we share more personal information—and we will share radically more in the next 10 years—it is becoming an increasingly important consumer rights issue, and I think that it will become a very hot political topic as well.

Lord Armstrong of Ilminster: So this particular statement is really more about the commercial use of information, rather than the regulation of it for security purposes.

Jamie Bartlett: It is, although the principle applies. There are huge levels of distrust, or very low levels of confidence in the Government, to handle carefully and responsibly people’s
personal information, for a variety of reasons. There have been some high-profile cases, which we all know about. So the principle is the same.

Lord Armstrong of Ilminster: So you think that the draft Bill in front of us does not achieve this degree of public acceptance, but that is in a sense not a defect of the Bill itself but of how it is being presented.

Jamie Bartlett: That would be my argument, yes.

Q725 Lord Armstrong of Ilminster: I think you also said that the public do not have a clear understanding of how personal data or information is defined. That is clearly an aspect of the same problem. Could you rank communications data in terms of intrusiveness and differing safeguards for access?

Jamie Bartlett: That is the task of this Bill, and why I argued that it might be widened out. The distinction is blurred between personal information and aggregated behavioural data in the minds of the public, and it is not totally clear. In our survey, we found that people tend to make a distinction between information that allows you to be directly identified, such as your name, address and e-mail address, and what you could call aggregated behavioural data—the stuff about your shopping behaviour and which websites you have visited. On the whole, people on average do not consider that to be personal information; between 40% and 60% think that that sort of information is not really personal at all. That is significant, because the system of regulation here must define and measure the harms involved in intruding on people’s personal space and their private correspondence and private lives under Article 8, and manage those harms effectively. The problem is that I do not think that there is a clear understanding of what the harms are, the extent to which certain kinds of access count as intrusive, and the extent of that intrusion. That is why there is a huge difficulty here. A practical example—I have given one with directed surveillance online—would be entering a Facebook group. There are plenty of closed groups that people within those closed walls consider to be a private space. What is the regulation that covers when agents of the state enter into those and collect information? I am not sure that RIPA really covers that adequately or that this Bill does so, but to me those are much more pressing issues. So there is a way in which we can begin to start to define different types of communications data and personal information on a scale, but it is very difficult to get a true handle on that because we do not have a sense of what the public really think about these things.

Q726 Lord Armstrong of Ilminster: If I may press this point, we have been told that a distinction is made between subscriber data, traffic data and user data. Would the public be more concerned with one rather than the other? Do you think that the Bill would be more acceptable to the public if its scope was confined to one or two of those data types but not to all of them?

Jamie Bartlett: I shall try to answer what I think, but I cannot say that I speak on behalf of a broader public consensus, as I mentioned before.

Lord Armstrong of Ilminster: I think we accept that.

Jamie Bartlett: But that is important, because a lot of people claim to speak about what we think and it is not always clear. I believe that it is less intrusive with regard to traffic data and that fewer harms are entailed, and that there are fewer risks to people’s privacy, than with use data, which is about websites that you have been visiting and your browser history. I consider
the latter to be more intrusive than the former and consider subscriber data to be more intrusive still, because that essentially means access to people’s personal information. I do not think that it is entirely accurate to lump them all in together as one data set, with the same level of intrusiveness, oversight and regulation required. That is my personal view.

The Chairman: Subscriber data, at the moment, are supposed to be the lowest level of intrusion, but you are suggesting that a mobile phone, tracking and recording where you are every five minutes of the day is quite intrusive.

Jamie Bartlett: It is measured partly by the harms that could come from agents of the state having access to that data. That could be considered, and I would consider it, potentially to have significant harms.

The Chairman: I am conscious that we are only on the fourth question and we should hear from Lord Carlile, but we have been delayed a bit by a Division. If you are going to give us a paper on a sliding scale, do you have a view or do you have a paper on the data for different levels of intrusion? Perhaps you could rank in that paper the things that you think least intrusive and those you think more intrusive.

Jamie Bartlett: In the paper that I wrote with Sir David Omand, #Intelligence, we drew some analogies between what might come under RIPA of online surveillance.

The Chairman: The Committee would find that very helpful, because we are agonising over whether we should look at revising the different scales of intrusiveness and whether we have got it right in the Bill.

Q727 Dr Huppert: Thank you. I was going to talk about #Intelligence. Congratulations on some of the ideas in that paper. You may or may not know that there is a master’s student at King’s College, London, called David Gray, who in his master’s thesis makes some interesting comments on how the six principles that you address fit with the Bill. He is somewhat critical, but there we go. One thing that I was particularly interested in was on page 42, where you say: “As the intrusiveness of the kind of SOCMINT increases, the causes for which it can be legitimately used must decrease”. You go on to talk about publicly available tweets, stuff that people intend deliberately to broadcast, and give a relatively long list of things that is slightly shorter than that in the Bill. We have been talking about authorisation levels for different types of data. Would you apply a similar principle, and which of the purposes in the Bill would you get rid of?

Jamie Bartlett: On reflection, because I have been thinking about this question a bit, given the importance of public acceptability and some form of consent, and given the often unknowable long-term potential misuse of technology to collect, analyse and use this information I would probably go along with the other witnesses in arguing that it should be rather limited. Public health, for example, is a good way in which very valuable information that can be used with communications data and other types of information for public health benefits. But the concerns that the public has about the potential misuse about this quite rightly mean a much more limited approach. There is a big distinction between open-source, publicly available, non-intrusive data, which is widely available to researchers, academics and commercial companies, who are not collecting this data but are using it. Some of that is communications data, too. There is no reason why the Government should not be allowed to access that, and I do not think that there should really be any limits on the agencies that can access that kind of information. But it should be done according to quite strict research ethics, taking great
concern over the possible harms to research participants and being stored very carefully. That should all be set out separately. I call it open-source, non-intrusive social media intelligence. For public health purposes would be a perfect example that you could use—the classic example is Google search terms to understand better how epidemics spread. But beyond that, for the purposes of intrusive intelligence of this type, I would have it much more limited. I would not really like to go in and say exactly which agencies I would take off or for which purposes I would remove it, but I would suggest a minimalist rather than maximalist approach.

Q728 Dr Huppert: If you do have any thoughts on this paper that you are sending, that would be useful. There are two other things that I wanted to raise. On your earlier comments on the amount of information that there is out there, I presume you would agree that one of the key things is not just about regulation—it is about teaching people about the value of data and what they can reveal. When you produce the paper about the hierarchy of different things, it would be very interesting to understand whether you think that they are well defined categories at all and to have your thoughts on the overlap between content and the different categories would be very helpful. We would all be very keen to avoid a situation where a police force, or whoever it is, believes a political type of thing to be one sort when there is a strong case that it is another sort, and you retrospectively go in and discover that there is a massive hole. The only way in which to avoid that is to have strict definitions, so that it is clear to everybody what traffic is, what use is, what subscriber is and what content is. It seems to me that there is a huge overlap—but your thoughts and comments either now or in written form would be very helpful.

Jamie Bartlett: I will put something together in the paper, in the interests of time, although it is worth mentioning that the scale of data acquisition technologies available now, often for free or for practically nothing, means that there is a huge democratisation in the ability of any agency to conduct huge social media monitoring. That is really important, because there will be occasions where police agencies and others will probably inadvertently breach things like RIPA without realising, because there is no clear definition of the extent to which certain information is personal or otherwise. You are absolutely right that there needs to be a clear distinction between the three data types set out in this Bill. What I will try to do, and I think that it is very important, is to collect as much available polling data as I can about public attitudes to that, because it is a big part of what is missing here.

Q729 The Chairman: I am sorry to interrupt, but I believe that some of the telecoms companies said that they did not understand the talk about the gap because there was a lot of information there if it was known how to access it. They say that it is in the public domain already and that the police and others need to be trained better to find the stuff that is there.

Jamie Bartlett: Yes, it is. The collection, acquisition, analysis and use of large, automated social media data sets of this type throws a big challenge to these agencies, because it is very hard to turn that into actionable, usable intelligence. It is good information and it might provide you with something, but a lot of it is misleading; rumours are rife and there are problems with the collection and analysis of the data. We are only just starting to understand the scale of that. Therefore, there needs to be a huge increase in investment in making sure that social media intelligence becomes part of the collection of tools that intelligence agencies
have, but that is why it needs to be regulated—because we need to make sure that there is public understanding about what can be done, why, under what conditions and by whom. So there are two sides of this. One is regulation to put it on to a legal footing, which is the basis of all of this, and which is why I do not think that analogies with China, Iran and Kazakhstan are very helpful. We regulate the ways in which privacy is breached in a way that those countries do not, even if they use some of the same technologies, which they do already, for all types of snooping. Also, there needs to be that way in which the police know what they are doing, so that we do not have the risk of inadvertently breaching various regulations, which is probably easier now than ever.

Q730 Lord Faulks: You have been very modest about speaking for the people, and the public. In describing your think tank, you say that the focus of your research includes “citizens’ juries, deliberative workshops, focus groups and ethnographic research”. What is ethnographic research?

Jamie Bartlett: Ethnographic research is a particular research methodology whereby you try to embed yourself in a community of people to understand their day-to-day interactions and their life as it is lived over a period of time, as well as the relationships and social dynamics, rather than just peering in from above as a researcher and trying to understand from a distance.

Q731 Lord Faulks: You say in the Demos report that the public “tentatively agrees with regulated, restricted access” within the context of social media intelligence. Given what you have already said about the difficulty of understanding the distinction, do you think that from your knowledge and experience that they would feel the same way about communications data, on the assumption that they understood that distinction?

Jamie Bartlett: Yes, I think that generally speaking there is broad support for regulated intelligence work, whatever that covers. What is important is that there is a proportionality and necessity test and due process—there is oversight and redress. The problem here is with the technicalities, which I cannot confess to understand entirely, which you need to understand to be able to decide whether those tests are being applied accurately. One of the most important things about this Bill is to have utter clarity over some of the technical aspects of it, which is what the witnesses here, particularly from the privacy groups, have done well to highlight—some of the areas where more clarity is needed to allow us to understand whether there would be broad support for the measures that are taken in this Bill. The general principle of regulated access to people’s communications data and to content is a fair one.

Lord Armstrong of Ilminster: And to content?

Jamie Bartlett: Yes, as it exists currently. One problem with RIPA as it stands is the perception that it has been misused and that the necessity and proportionality tests have not been effective enough. There is a need, as I have stressed before, to be quite minimalist at this point with this type of intelligence, because of all those unknowns—about the ways in which technologies will change and about understandings of different types of privacy. In that case, it is important to be minimalist rather than maximalist.

Q732 Mr Brown: We touched earlier about the need for a public debate, if only to inform our fellow citizens, and in your evidence you mention the need for a Green Paper. Would you say
to us that we should have a Green Paper on this Bill, which is currently subject to pre-legislative scrutiny, even if that meant delaying bringing the Bill to its formal Commons and then Lords reading?

*Jamie Bartlett:* Probably, yes, simply because what is really important about communications data now and other types of internet-based content is the extent to which it is woven into everybody’s everyday lives. It is so important for everybody; it has a huge economic and social benefit to the nation. The internet is worth billions to the economy and has value in terms of social and economic well-being. One of the first of the three public goods that I mentioned that has to be balanced is social and economic well-being, which could be detrimentally affected by an overreaching surveillance system. Given all those factors and the fact that the Bill has been quite inaccurately described by many commentators on it, I think that it is probably essential, because public consent is ultimately necessary for measures of this type.

**Q733 Lord Strasburger:** You may feel that you have answered this question already to some extent, but do you have any concerns that in the area of data communications and social media there is a need to train law enforcement bodies in the use of such data if any new powers are to be effective?

*Jamie Bartlett:* As I mentioned before, inevitably the intelligence agencies and police have spent many years developing capabilities in human intelligence, signals intelligence, imagery intelligence and all sorts. This is quite new; it is prone to great mistakes, and it is very difficult to analyse and difficult to draw predictive models out of these huge data sets. Commercial companies are spending millions and millions of pounds training analysts and developing methods to do this really well, and police agencies should be doing the same, although not necessarily to the extent of these commercial companies. But clearly being able to use social media and CD intelligence is actually rather difficult and requires, as ever with a new form of communication, training and capabilities to analyse it accurately.

**Lord Strasburger:** So there is a suggestion that those agencies are not currently equipped to deal with that massive volume of data.

*Jamie Bartlett:* Some of them are, but some of them probably are not. Remember that local police constabularies are also able to tap into all this data as well. GCHQ probably has incredible analysts who do all sorts of fancy things that I have no idea about, but it could be relatively low-ranking police officers who also have to get real-time data and decide deployment very quickly on the basis of some social media intelligence. That is actually quite difficult to do. Given the difficulties involved, and the sorts of people making decisions on the basis of this, it could be done better. You only have to read the report from Her Majesty’s Inspectorate of Constabulary about the riots to see that. Resources should have been put into turning information from these data sets into intelligence—to validating and verifying it and then using it. That was the problem.

**Q734 The Chairman:** But you are not suggesting that there needs to be a new level of regulation? If somebody says through his Blackberry, “Let’s go and riot in Tesco tonight”, the police surely will not need regulations or controls before they can act on that. Are you just suggesting that it is real-time information and that they should be better equipped to exploit it?
Jamie Bartlett: Well, it really depends where that data has come from—and that is the problem. On social media sites, there is a huge variety of different platforms, some more private and some more public than others. A very low level of authorisation is required for some of this, but some kind of measure would be helpful to reassure the public that this is being regulated in some way, even if it is extremely low. As I mentioned before to Dr Huppert, that could just be basic ethics about how you look at open-source data.

The Chairman: Are there any other points for Mr Bartlett? Thank you, that was absolutely excellent, and thank you for the paper that you have already submitted. We look forward to the paper on the sliding scale and your ideas on the levels of intrusiveness. Thank you very much, I am sorry we are running a bit late.

Jamie Bartlett: Thank you.
Lord Carlile of Berriew (QQ 735-749)

Examination of Witness

Lord Carlile of Berriew, former Independent Reviewer of Terrorism Legislation

Q735 The Chairman: Welcome, Lord Carlile. I am sorry that you have been delayed. We have had a Division and we tend to overrun in our questioning in any case. Just for the record, if you would state what you have been doing to keep yourself out of mischief in the past 10 years, from September 2001 to 2011, which is the main reason why we have you here.

Lord Carlile of Berriew: From 11 September 2001 until February 2011, I was the Independent Reviewer of Terrorism Legislation. I remain the non-statutory independent reviewer of national security in Northern Ireland, and I also remain the chairman of NICOP, our rather unhappily named Committee in Northern Ireland, which looks after close protection of judges and other senior people. So I am still in touch with the security world, albeit not as intensively as before.

The Chairman: Thank you very much for that introduction. The Committee is in awe of the work that you have done in the past 10 years, and the work that you are continuing to do.

Q736 Michael Ellis: I have been interrupted twice so far by the Division Bell when I ask a question, and it is about to happen for the third time. Could I just start by asking what your views are on the present law relating to the retention and acquisition of communications data, before I ask you about the draft Bill? The present law, you may well be about to say, was adequate when it was first enacted but, given the way things in this field move so fluently, it may not be as sufficient as it was when first given Royal Assent. Could you say something about your feelings about the present law?

Lord Carlile of Berriew: Well, you have asked and answered the question, really. I agree with the answer that you offer.

Michael Ellis: I was at the Bar for several years and cannot get out of the habit.

The Chairman: Order. There is a Division in the Commons. We will reconvene again as soon as we are quorate in Commons terms.

The Committee suspended for a Division in the House of Commons.

The Chairman: We are now back in public session.

Lord Carlile of Berriew: I think I wanted to say, although it may not be a direct answer to the question, that I view this Bill as an opportunity to tidy up and modernise the law in relation to communications data. It has had a very long gestation. I was asked by the last Government to advise on proposals that are very similar to the proposals in this Bill something like five years ago. A huge amount of work has been done on it, and actually this Bill addresses some simple, practical questions and provides better solutions to them, on the whole.

Q737 Michael Ellis: As we heard from the previous witness, Mr Bartlett, there have been reports in the media that do not quite connect with what you and Mr Bartlett have been saying. The media portrayal has been, to generalise a little, somewhat hostile towards the Bill’s
provisions. What do you have to say about that? Do you recognise what has been suggested in some areas of the media as accurate?

**Lord Carlile of Berriew**: No, I do not. I think that the term “snooper’s charter” is a complete traducement of the Bill. You did criminal work at the Bar, too, and I believe that this Bill deals with practical issues in that context. I can recall straight off the top of my head three criminal cases, all murder cases, in which I was involved as a barrister, which resulted in convictions, not solely but realistically on the basis of communications data of exactly the type that is being sought in regulation in this Bill. For one of those cases, there was difficulty in dealing with the communications data because of the non-standardisation of the information sets held by the different telecommunications providers. One compared, for example, O2’s records, which were in a different form from BT’s records, which caused evidential difficulties in the courts, but the information that was provided was absolutely crucial.

**Q738 Michael Ellis**: I take it from that that you do not consider that anything about the Bill would impede your previous responsibilities to carry out law enforcement functions? Could you also say something about the balance and what you anticipate would the correct balance would be between the individual’s right to privacy, which we all accept is important, and the need to access communications data for proper law-enforcement activities?

**Lord Carlile of Berriew**: Well, nothing in the proposals in this Bill would authorise the interception of content of a communication. If the content of a communication is to be intercepted, that is a matter of special application, which exists in another form.

**Michael Ellis**: That requires the Home Secretary?

**Lord Carlile of Berriew**: It does, and as I understand it the oversight powers for that kind of interception are being strengthened. Also, the very small proportion of RIPA requests made by local authorities, for example, which are often trotted out as the worst possible example of RIPA requesters, is now being regulating by limiting access to those applications that are approved by a magistrate. So I do not think that there is any weakening of privacy in this Bill. What is absolutely essential for the proper detection of serious crime is that the police should be able to know who was telephoning who, for how long and at what time, for example. That is used every single day in the courts, up and down the land, and prosecutions brought by the CPS in very serious cases would be brought to their knees if this was not possible. What the Bill does is to standardise the data sets and ensure that all the companies concerned know what they have to do.

**Q739 Michael Ellis**: Do you agree with Mr Bartlett, therefore, that there is a gap in the law at the moment that would be filled by provisions such as those anticipated in this draft Bill, which would serve to regulate the law enforcement agencies better than they are now and therefore protect the individual’s right to privacy, because it would be codified in a more collective fashion?

**Lord Carlile of Berriew**: Yes, and a very simple example is that some of the telecommunications companies keep this data for two years, whereas this Bill requires them to keep this data for one year minimum. They may keep it for longer and they may not, although I apprehend that they are likely to standardise and keep it for one year and then dispose of it or delete it at that stage.
Michael Ellis: Finally, the present law is said to be insufficient in two particular respects. One is that it does not cover providers based overseas, and the other is that it does not require providers to retain or generate communications data that they have no business need for. As you alluded to yourself, Lord Carlile, such data is used in the criminal courts on a regular basis, which has been available because providers have had to collate that information for their own bill-charging, in many cases. But now with advances in communications, not all that data is necessarily collated for bill purposes. Therefore, the proposed provisions in this Bill would require that. Do you recognise those two areas as holes in the provisions as they stand?

Lord Carlile of Berriew: I do. The question of business need must be considered, but there is a public need for this information to be retained for a certain period and, preferably, in a standard form. I do have some views about the scrutiny aspect of this. The Bill does not go as far as it could in dealing with scrutiny. On overseas providers, this is a difficult jurisdictional question and requires co-operation, dare I say it, particularly on a European front to ensure that information of this kind can properly be shared. We run into problems in courts over the different standards about communications data and intercept. For example, intercept is admissible in Dutch courts but not in English courts. I have been in a case, therefore, in which Dutch intercept was admitted in a Crown Court in Nottingham. That sort of anomaly needs to be ironed out on an international basis, irrespective of whether it is intercept or not.

Michael Ellis: But you support this Bill.

Lord Carlile of Berriew: Yes, I do.

Lord Strasburger: You have spoken passionately about the benefits of CD in law enforcement. I do not think that anybody is proposing any reduction communications data, but how do you feel about content being part of the data that are available to law enforcement?

Lord Carlile of Berriew: I am wholly opposed to data being made available routinely, and this Bill does not provide for content to be made available. There are cases, obviously, where content may be important, and there may be good reasons for making a proper application in due form to obtain it. It does happen, again, all the time, although to a much lesser extent than accessing communications data.

Lord Strasburger: That being the case, are you aware that this draft Bill takes us into technology areas where it becomes increasingly difficult to separate data from content, in particular but not exclusively when encryption is used? When encrypted information is decrypted, it is very difficult for those doing it to anticipate where they are going to find content and where data. Does that give you any concern at all?

Lord Carlile of Berriew: I was advised when I was independent reviewer of terrorism legislation that proposals in this kind would not result in content being revealed. I am not a technological expert. It is a matter for the Committee to assess whatever evidence it receives. It is important that when content becomes revealable, it should be filtered out and not seen by the authorities without the correct authorisation. This is akin to filtering out legal professional privileged information in a criminal investigation, which is now done routinely by people like disclosure counsel or employees of the CPS. It can certainly be achieved, it is just a question of having the right mechanism to deal with it. Typically, if somebody is arrested in a fraud case and computers are taken with millions of documents on them, the question of legal
professional privilege is dealt with separately before the inquiry team sees any of the evidence. I believe the same could be done rather more easily with this type of data.

**Lord Strasburger:** With the older technologies, with straightforward telephones, it is very simple to separate content and data, but in the environment that this Bill is moving us into it is becoming increasingly difficult in some cases to do that.

**Lord Carlile of Berriew:** I accept that if that is the evidence that the Committee has heard. Somebody will have to solve that problem, but it is not going to be me.

Q742 **The Chairman:** If I can pursue this point, I think we all agree that data such as who phoned who for how long, the telephone number and so on, are absolutely essential. As some of the evidence that we will hear when we move on to the internet suggests, if I log on to Alcoholics Anonymous, that page itself is in some ways content. It shows that I may have a particular interest in logging on to Alcoholics Anonymous, so it reveals content to some extent. Do you accept that, if that is the case, there is an element of content there that would have to be strictly regulated?

**Lord Carlile of Berriew:** Well, it is a very fine distinction, if I may say so. To take one case that I was in, the cell site analysis showed that my client was communicating with the man who she had hired to murder her husband. Her number was her numberand the recipient number was his number—the man who committed the murder. So one knows through other material who they are. If somebody logs on to a terrorist website, which is teaching them for example how to make a bomb, what is the difference? It is a very analogous process. I cannot see any difference, or why the originator and the recipient of a log-on should not be disclosed in the same way. Obviously, the scrutiny process is extremely important to make sure that it is not abused, and I have some reservations about the extent of the scrutiny process in this Bill.

**The Chairman:** We shall come to those in a few moments—we will not miss them out.

Q743 **Lord Faulks:** I think that my question has been covered, but I shall ask a different question. If this Bill becomes law, CSPs will have to retain information that it is not in their commercial interests to retain. From your experience, both as independent reviewer and a barrister, do you think that this information is likely to be useful?

**Lord Carlile of Berriew:** Probably not, in most cases. In the occasional case, additional information will be useful, but it is the raw data of the kind that we have been discussing and which the Chairman mentioned just now that is of real value to the authorities—the communications data, which is what this Bill is all about.

**Lord Armstrong of Ilminster:** I think that the point I was going to make about content have been covered.

Q744 **Lord Strasburger:** The Home Secretary and the Justice Secretary have said that 25% of the communications data required by the police and agencies can no longer be acquired. Is that your experience?

**Lord Carlile of Berriew:** I have no basis for confirming or denying that—I do not know. I have not done that statistical exercise. I accept what they say.

**Lord Strasburger:** You do?

**Lord Carlile of Berriew:** If they say it, I accept it. I presume that their statistics are broadly correct. I have no reason to doubt what they say.
Lord Strasburger: Are you able to share with us any instance where this inability to access data has impacted on the conduct of an investigation or the prosecution of a case?

Lord Carlile of Berriew: Well, if there is data that is not available, plainly that is going to impact on an investigation, but if 75% of the data is available, unless those committing crime have a very peculiar knowledge of what is unavailable, there is, logically, a 75% prospect of the necessary data being available. My experience, such as it is, over the last 42 years of criminals of all shapes and sizes, is that they are nothing like as clever as you would imagine. You would be surprised how many serious criminals make phone calls on lines that are listened to or send text messages that can be tracked and retain them in their telephones so that when they are arrested all the police have to do is to switch the phone on and start scrolling.

Lord Strasburger: So you are not aware of any particular instances.

Lord Carlile of Berriew: I am not aware of any particular instances, but I am sure there will be instances where people have used a provider whose system cannot be traced in the same way. But even if 25% of information cannot be traced in that way, if the inference is that we should not bother with the other 75%, I would reject that out of hand as being illogical.

Lord Strasburger: I do not think that is the inference. The Minister for Universities and Science told us that the number of communications services providers subject to data retention obligations is and will remain a fraction of the providers in the UK. Does that surprise you?

Lord Carlile of Berriew: It does surprise me, because under Clause 1 of this Bill, indeed under this Bill generally, my understanding was that requirements to retain data could be extended to other providers. Am I wrong about that? I do not think so. So it is the duty of the Home Secretary, or whoever is the responsible Minister, to find out who the relevant providers are and add them to the list. It is done by order under the Bill, so there can be a prayer against if anyone thinks that appropriate.

Q746 Lord Armstrong of Ilminster: Can I ask about that? If we were to suggest that these powers should be confined to data that these companies hold for their own business purposes, do you think that that would go a long way to meeting the requirement? There would be some data that they would not get. But if we were to say that it would be a good idea to confine the requirement to hold and store to those categories of data, which they in any case hold for business purposes, for no longer than three or six or 12 months, as in the Bill, that would get
us a good long way towards achieving the purposes of the Bill, and possibly help to calm public concern about privacy.

**Lord Carlile of Berriew:** It would defeat the purposes of the Bill, if I may say so. Businesses will determine for themselves what they require to retain for business purposes. Billing processes in mobile telephony are becoming ever more sophisticated day by day; companies wish to retain less and less, because retaining things costs money and involves people working—usually quite well paid people. Therefore it is the responsibility of the Government to decide what set of data needs to be retained, of the kind that we have been discussing, and then ensure that the companies retain it.

As to the second part of your question, I am not optimistic about calming not public opinion but the opinion of people who have been prepared to talk stridently against this Bill, because by and large it is extremely ill informed and inaccurate. Only an optimist would believe that a particular group of people could be persuaded that this Bill was actually relatively harmless and positively helpful to the public interest. Parliament has to be brave about this, bearing in mind that successive Governments have seen the necessity of introducing this legislation. It is not really a party political issue at all, or at least it should not be.

**Q747 The Chairman:** Lord Carlile, can I go back and press a question that Lord Strasburger asked. He said that the Minister for Universities and Science had said that the data retention obligations would impact on only a fraction of the providers in the UK. You answered that by saying that Clause 1 allows it to catch everybody. That is part of the problem that we have been wrestling with. Some of the communications providers, the telecoms operators said, “We don’t know what the Government want. Clause 1 is massive and could involve everything under the sun, but privately the Home Office says not to worry and that it will only be very light touch and only a few people will be caught”. What I am trying to get at is that in the advice you have given successive Governments, can you share with us what the real target is and how extensive the orders might be? Will it be more than just the big six telecoms operators that are caught?

**Lord Carlile of Berriew:** The first piece of advice that I gave maybe 12 times a year to successive Governments is that they have to be much better at narrative. The narrative over these proposals has in my view been inadequate. There has been a much stronger counternarrative. So I think that the Government, or successive Governments, could have told a much stronger story. The Government and industry need to be seen to co-operate. It should be made clear that what is being aimed at here is to ensure that the necessary data from all equivalent providers, whether they are large or small, are retained for a period of 12 months so that it can be investigated by the investigating authorities when it is appropriate and proportionate. That really is the simple message that has to come out. I believe that any Government—and you as a former Chief Whip know how defensive large political parties, at least, are—

**The Chairman:** We are all in this together.

**Lord Carlile of Berriew:** It is entirely understandable that the Government for the time being have no appetite for suddenly opening a new warehouse full of data, because that brings down criticism like a ton of bricks. We can reasonably expect any Government, whether there is a change or not, to be cautious about the number of orders that it lays to extend these provisions. I think that is a realistic view.
Q748 The Chairman: Finally, you have talked about the Government and the industry needing to co-operate and be seen to co-operate better. Would it surprise you if I told you that we have had evidence from many of the big telecoms companies saying that the only discussion that they have had with the Home Office were in the few days before the Bill was published, or the day after, and some of them said that the first discussions that they had with the Home Office came after we summoned them to give evidence in this Committee?

Lord Carlile of Berriew: It would not surprise me in the least, but it should surprise me.

Q749 Lord Faulks: See if you can compare, if you would, the role that you performed as independent reviewer of terrorism, looking among other things at control orders and their successors, and the role of the Interception of Communications Commissioner, who has a different role in relation to these communications. Do you think that his powers, or her powers—because he is about to be succeeded—are sufficient or could be improved or supplemented?

Lord Carlile of Berriew: I think the powers are sufficient. I think that there is a difference of perception. The Independent Reviewer of Terrorism Legislation, either me or my extremely good successor, David Anderson, carries out a very public role. The public nature of that role is reassuring to some and, to use a neutral term, satisfying to others, because at least they have something to criticise. The lack of public face of Sir Paul Kennedy’s role—he is a friend and I have huge respect for him—is a difficulty. That is why I would like to see a slightly different form of scrutiny in this Bill.

The Chairman: Lord Carlile, are you able to give us another 20 minutes? In that case we will suspend for a vote in the Commons—and please will Commons colleagues come back as soon as we can and we will crack on. But if we are going to be inquorate, we cannot continue. I am sorry about that, because by hook or by crook we want to get a bit more from you, which we will not be able to take today. I suggest that we will try, Lord Carlile, to find a 15-minute slot at your convenience, if we can, just to get a little bit more on scrutiny. If not, perhaps we can send you questions and you can give us written answers.

Lord Carlile of Berriew: If you can send me questions, I will reply to them.

The Chairman: In that case, the Committee is suspended.
TUESDAY 23 OCTOBER 2012

Members present:

Lord Blencathra (Chairman)
Lord Armstrong of Ilminster
Lord Faulks
Lord Jones
Lord Strasburger
Mr Nick Brown
Michael Ellis
Dr Julian Huppert
Stephen Mosley
Craig Whittaker
David Wright

Henry Porter, Duncan Campbell and Paul Heritage-Redpath (QQ 750-783)

Examination of Witnesses

Witnesses: Henry Porter, Columnist for The Observer, Duncan Campbell, IPTV, and Paul Heritage-Redpath, Product Manager and Solicitor, Entanet Opinion, examined.

Q750   The Chairman: Gentlemen, thank you so much for coming to give evidence before the Committee today. Clearly, the Bill we are considering has provoked a wide range of interest and some comment in the press, and we wanted to make sure, before we concluded our evidence-taking sessions, that we gave members of the press an opportunity to tell us about the Bill and their perceptions of it and their views on it. We are very grateful. Now, although we know who you are, it would be helpful, please, if you just introduced yourselves for the record.

Henry Porter: I am Henry Porter. I am a novelist. I work as a contributor for the Observer and I am London editor of the American magazine Vanity Fair.

Paul Heritage-Redpath: Good afternoon. My name is Paul Heritage-Redpath. I am a solicitor and a product manager for an internet service provider called Entanet.

Duncan Campbell: I am Duncan Campbell. I have been an investigative reporter for 35 years and I have also been an expert witness on communications for nearly as long. Over the last decade, I have extensively audited and tested communications and computer data in the criminal courts. In terms of my journalism, reports that I published in 1980 and evidence I provided to the European Court were part of the trigger for the judgment in Malone v UK, which led to the Interception of Communications Act. Much later on, I was the expert witness and instructed by your next witness, Keir Starmer, in the 2008 European Court case of Liberty & other organisations v the United Kingdom. I have made sure that a copy of that case is in the hands of the Committee because it specifically considered issues of filtering in the context of communications collection and analysis and found the UK’s practices to be non-compliant.
The Chairman: Excellent. Thank you very much. Our Committee members will have a range of questions for you. Do not feel you all need to answer every single one unless you wish to, but again do not be constrained and hold back.

Q751 David Wright: A gentle opening to the bowling, if you like, to ease you in at the crease. The media coverage of this proposed legislation has been, I think you could say, unrelentingly negative. It has been described as the “snoopers’ charter” by many. Do you think that is a fair analysis of what has been proposed, because we have certainly taken evidence where witnesses have said they felt that the media coverage relating to this Draft Bill has been inaccurate?

Henry Porter: I do think it is fair, because I think it is a very bad Bill and it threatens the very foundations of our liberal society, and if you come from where I come from, which is a profound belief in our democracy and the ways of a free society, you see this Bill as a very great menace to it. So, even if the coverage is unrelentingly against this Bill, I do not think it is necessarily unfair.

The second point I would make on this is that we have to hold Government to account. Now, the media often comes in for a lot of flak itself: the BBC today, newspaper journalism throughout this last summer and last year. But the fact is we still have this important job to do and it will make it a great deal more difficult to do this job if the communications of sources in Whitehall, in politics, or in big companies can be traced to journalists. So that is another reason, and perhaps the secondary reason, why the media is probably very against this Bill, but I would say that the first reason is that it is hostile to the sort of society that we have now.

Duncan Campbell: I found it difficult to hear the Home Office complaining of unfairness when what they are putting forward to Parliament and this Committee is something that has really been stewing around for at least 10 years, being pushed forward in various ways, and yet when the witnesses come here it seems that no one in the telcos knows what they plan to do or how they will implement it. I was also gravely concerned that Mr Farr in his evidence, and within almost his first interchange with Mr Ellis, completely misled the Committee about the situation with communications data. I put a note in to expound on this should it be necessary, but the statement that 30 years ago BT was collecting communications data, and the implication that they will now not be making that sort of information as available, is the exact opposite of the truth. So, he is extremely badly informed, and passing on poor information and misrepresenting the situation as it is seen now in terms of the amount of information that is available, which has been increasing. It has been increasing as devices become available and new forms of data, for example location and cell-site analysis, come into the system. So I see the Home Office as having mis-served itself very badly from the very title of the presentation of the Bill as remedying a gap. No, they are not. Perhaps proportionately there are things that could be done, areas that can be addressed, but they have left themselves wide open to this accusation of it being a snoopers’ charter.

I would not quite endorse that title yet, because what they are creating, if Parliament were to give them the powers in this form, would really be a universal surveillance engine attached to the mass or all of the British internet. Now, what you do with it, and whether it does become a universal snooping engine, is withheld from us, because none of the orders, none of the codes of practice, none of the facilitating instructions, some of which may come to Parliament, some which may remain classified, are before us. So, again, given the degree of obscurity, the surveillance engine could be the snoopers’ charter or it could be reined in.
I would just, finally, say that the important point of human rights, which seems to have been overlooked in the way the Bill was drafted, has been formed. It has been formulated for us by the European Court and really supports the apprehension that perhaps is seen as coming too stridently from some journalists. “The mere existence”—and I am quoting now from the judgment—“of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users,” which is Henry’s point and I would absolutely and strongly endorse that for the special case of journalists seeking confidential sources and secure communications to them when those sources act and come in the public interest. The Court finally said the mere existence of legislation of this type is an interference with Article 8 rights irrespective of whether there were to be measures taken against an individual person. So that is a very powerful legislative Act, longstanding in the European jurisprudence, that really does go to help understand why epithets like “snoopers’ charter” have had widespread currency.

Paul Heritage-Redpath: I would say that the newspaper coverage has been, if anything, relatively balanced on this issue, because this is something that strikes at the heart of human rights, and I do not think the Home Office have done themselves any favours in the way that they have presented or engaged with it. I think the newspaper coverage has been limited by the fact that it is quite difficult to articulate to the public what lies behind this Bill and I believe that is a deliberate intention.

As a communications provider, we have had no contact from the Home Office. As a member of the association of communication providers, we invited the Home Office to speak to all of us collectively. They spoke for half an hour and they told us absolutely nothing more than you would find in the Notes on the Bill on the grounds of national security. Now, this is something that strikes at the heart of how we operate as an industry, and I think the fact that they will not articulate it to us means that the press articulating that to the public is very difficult.

Q752 David Wright: So your view, as a panel of witnesses, would be that far more groundwork could have been done by the Home Office in terms of background detail. One of the things we have struggled with as a Committee, Mr Campbell, relates to your point, which is about understanding what lies beneath this legislation: what will come to Parliament at a later point?

Duncan Campbell: Yes. I can address it both as a journalist and I can address it from the bottom of the pile, if you like. What is it that my police colleagues would like to be bringing into court that they could get from communications data that they do not now get? There are relatively few things, given the richness of material from other sources, and if you take, for example, whether we can go to Skype, it has been laid out that there is a completely alternative route for going to Skype, so we do not need to worry about Skype in this context.

They have also eschewed looking at things that could be simply explained to Parliament and public. Way, way, back, 12 years ago, we were working on Chapter 2 of RIPA and soundings were taken, views were expressed, as to how you proportionately apply the surveillance of weblogs. Chapter 2 of RIPA does provide some powers, but it has never really been put into practice. Now, since the new provisions, excluding the additional filtering requirement, necessarily embrace all of that, that whole debate could have been laid out in the open. The
Home Office could have briefed on it, they could have addressed the arguments that were put for both sides then, expressed a position, allowed Parliament to take its view and so on and so forth. So they have missed a lot of areas where, without needing to have recourse to national security considerations, they could have been open.

Q753 Lord Strasburger: I was going to ask you why you think the Home Office have got it so wrong.

Duncan Campbell: I think they have insulated themselves too much into a very small group that really only essentially talk to themselves and a few others, a few key engineers, and not sought to access even, perhaps, their own Ministers in getting an understanding of what might be required and what might be developed. They are operating in too small a world. I went myself to one of the Home Office briefings a couple of years ago when we were looking at the previous Bill and asked them to try to explain some simple points, and they struggled. They did not seem to know their brief and they did not seem to be very enthusiastic about learning their brief. It was very disappointing.

Paul Heritage-Redpath: Speaking as a member of the public, there was an extraordinary self-assurance about the presentation by the Home Office to us of a from-high-to-low basis: “We have decided this is in our best interests, and we are not going to tell you what it is; you will just have to believe us.” That was really how the Home Office presentation, at a quite senior level, came across to us.

Q754 The Chairman: You said in your opening remarks, Mr Campbell, that there are areas that could be addressed. It would be helpful if you could elaborate on those for us, please.

Duncan Campbell: First of all, I referred to weblogs. Now, internet service providers do not routinely obtain a log of what happens when a user, any one of us, is using our browser. In fact, a very rich trail of information is generated, many entries per page, on your computer, and for a certain time it would also be held by the communications service provider. So a step that the Home Secretary could take is, by order, to have that data held. It would be huge; it would be difficult to process, but we all know what it is. It comes into the courts every day, because it is also found on suspects’ and defendants’ computers. So it is a kind of evidence that need attract no secrecy. The businesses do not want it because beyond, say, a few weeks to do an engineering study of whether your server is working, you absolutely do not want to store that kind of data. But there need be no secrecy about those kinds of records or how they might be filtered or how they might be used and, indeed, the previous debate on RIPA addressed that. I think Professor Anderson’s evidence also covered some points about that and probably Professor Sommer’s too.

Then there are those areas where the solutions cannot exist realistically. The Information Commissioner mentioned virtual private networks; I would agree with that. There is the problem of Tor. It is a problem from the point of view of UK law enforcement, but, although I did not put it in my CV, I go and work for the other side on occasions, in that respect, bringing the knowledge of what you can hide. I have done that quite specifically in support of the Syrian insurrection and people who are struggling to overthrow the Assad regime and, of course, they have high dependency on Tor, their lives are at risk and if this Government were to, by some method—and I think Tor would say it is impossible—make that not available to them, we would bring about a far greater deficit in human rights in other parts of the world.
You have things like Skype, which have set out a model that works if you address the mutual legal assistance treaty things, and I have seen products come into the courts from MLAT. It is effective; it is what you want; it is the communications data that is asked for. All of that is not being considered.

Q755 The Chairman: There are criticisms that MLAT is a bit slow.

Duncan Campbell: I have never seen MLAT work fast, but I think already comments have been made as to the way the Foreign Office could be encouraged to speed that up.

Q756 Lord Strasburger: You talk about the request filter. Is it the case, in your view, that the distributed database that this Bill foresees combined with the request filter is going to be any different from the centralised database that was proposed in previous legislation?

Duncan Campbell: It appears to be larger, notwithstanding that it is distributed. I say that because the centralised database would ingather the communication service providers’ records at the specified times and hold them nationally with, no doubt, automated access, and that is required to come into being by the first part of the Bill. So basically, you have the national database within the Bill anyway, save that it will be held, in this model, by the CSPs. You then layer onto that the DPI devices that will hang on the key points of the United Kingdom network and mine as yet unspecified classes of data, presumably into similar local databases, but they will, by their nature, have to be integrated nationally, and I think this was conceded by the Home Office witnesses. You are going to data match across things that you see in the content derived from different nodes on the internet with different companies in order to try to get a match to generate communications data. So, if that analysis is correct, this is the national database of the previous scheme plus the additional databases supporting the need to retrospectively look at, I would imagine, a year’s data taken from whatever the filtering system turned out to be. So, a bigger database.

Paul Heritage-Redpath: If I may address the Committee on the request filter generally, I think one of the challenges in the discussion around this debate is that it goes to technical matters and there has been very little technical discussion. The web is, ultimately, ones and zeros, and they are aggregated up into chunks, and those chunks may or may not have some meaning. Now, from the point of view of the request filter, we can see that use of the web is continually increasing, so the database that we are talking about, even if you take a year’s slice, is only ever going to get bigger. Wherever that database is housed, it will require space, cooling, power, maintenance and people, and even if the Home Office pay ISPs for those things, that affects how you run a business, because you have to allow for somewhere for that database to live. Also, the more people and the more data involved, the more risk there is of human nature going in and having a look. This would be an extraordinarily large database. Keeping it secure would be, in my view, almost completely impossible. It is easier from a technical perspective than a simple “who is able to access this data?” perspective. So, from that point of view, it is a huge, huge risk, and I speak as somebody who looks after data centres and looks after ISPs.

It is unfortunate that we all have to speculate, because we do not have clarity on what is intended. I think, from what I and others have read on the idea of the filter, it is Google for a set of databases that have been collected about traffic, so it can make connections. Now, on a very small scale, something similar has been tried recently by the Motion Picture Association.
of America and the BPI. They looked at about 13,000—so a small sample—of requests where they thought traffic looked like people infringing copyright, and they used an automated filter to perform that exercise. In 16% of cases the IP addresses of the infringers were ones that were inaccurate, either malformed or not the right people. That is a very small sample. Now, that is just sending letters about copyright infringement, so it is not going to ruin anybody’s day too much, but if we scale that up to everybody’s communications all the time and have that sort of error rate or even a very small error rate, then the risk to human liberties is significant.

I would ask the members of the Committee to think about when you do a Google search. Bearing in mind that Google have the best engineers on the planet working full-time on search, how often when you enter a search term do you get a single correct result? You get many results and sometimes they are right, but how often do you get a single correct result? So if the idea of the filter is to say “We have aggregated traffic from all sorts of providers and we are then going to run a filter,” what are the odds of that filter being 100% accurate and, even if it were, what is the use to the Home Office when they go before a court and say, “I have evidence, but I cannot tell you where it has come from because all I have used is a filter. I do not know what the filter is filtering and I do not know if it has got it right.” So, from that point of view, just as a commonsense view, I have real problems with the filter.

Henry Porter: I would just add that it would be lovely if we could start using plain language here. This is a search engine or a data miner. I am not, obviously, as technically expert as these two, in fact, much, much less so, but I had to scurry around and ask people who do understand these things for an explanation as to what it is. What it is is a data miner, so let’s call it a data miner, which makes very, very fast connections between numerous sources of information. The fact that it is not in one silo of information does not make the slightest bit of difference. It is giving to a small group of people access to a massive amount of power. When we talk about this filter, we are talking about computing power, and it is computing power that is increasing with an astonishing acceleration every year. Our ability to do things tomorrow that we could not do today is extraordinary. So this Bill, apart from anything else, should take into consideration the massive power that will be given to these people who are running this system under the communications data silo or whatever you like to call it. So I would just warn that this is not power of today, but power of tomorrow. Who is going to be in the Government? Who is going to be in charge in the Civil Service? These are the things that worry me, the non-technical expert.

Q757 Lord Strasburger: This is for Mr Campbell specifically. Back to the filter. We have had evidence querying whether the results from the filter will meet evidential standards. If you were working with defence counsel on a case that relied on filter results, how would you go about questioning the admissibility of evidence derived from the filter and the weight to be attached to it?

Duncan Campbell: Lord Strasburger, my expectation is that the courts would probably never get to see the kind of information passed out of the proposed request filter. I will explain why in a minute, but the obvious point that goes to is how useful this can really be for prosecutions. The evidence given specifically in Liberty v the United Kingdom was that we are not going to discuss filtering, it is too complicated, you will not understand it, it is all classified, and we are not going to reveal our methods. The main reason for doing that, I
suspect, is that the driving problem—which they never quite admitted until they came here and said, “We are never going to get one in six communications”—is that they do not want people to figure out what it is that they cannot get, because, fairly obviously, the bad guys will navigate through that. So their clear position in *Liberty v the United Kingdom* was that they do not want to explain how filtering works and they are trying to protect not their strengths but their weaknesses.

If I was wrong on that—I could be—then the admissibility would depend on the way that the court would approach testing, for example, an assertion from the prosecution by its experts that our filters had shown that somebody calling themselves Santa Claus on a certain network was, in fact, an individual they could identify and had in the dock. They would have to be prepared to disclose, in that case, the details of their filtering processes, which communications service providers they were taking it from, how they were pulling down the data—that is the phrase they used in *Liberty v the United Kingdom*—and say how they make it a match.

Then it gets worse. Obviously, if one is instructed for the defendant who contests that match, it would be necessary to do an audit trail according to the recognised standards of computer evidence to see what the parts are that go to make up that match. It may be statistical. It may be quite complex, and defence counsel will expect and the judge will expect that the prosecution, before bringing that evidence, will consider whether there is alternative evidence that you would wish disclosed, or at least to consider you had to disclose, to protect the rights of the defendant to due process. These are the obligations under CPIA and the Attorney General’s guidelines. The defence, through the court or otherwise, might, quite properly, wish searches to be done of a more extensive sort. We would put in our own filter requests and get yet more pieces. You can, I think, start to see that, were you to add to the existing complexity of computer data cases from which judges, quite reasonably, resile if they have to instruct juries, you would have an immense porridge of bits and pieces gathered from around the network, and an algorithm written by one company for the Government might say, “Santa Claus, 87% probable to be Mr Hoskins,” for example, and, on the other hand, an alternative analysis might say you have not got a case that you have identified this person.

There is also the problem that, if you go back over the implementation of RIPA, they have not really stood up to evidential standards. Early on, we did have issues about whether the computer data—and it is computer data—that comes through in response to Chapter 2 requests—subscriber calling, bill data, cell-site data and so on—should be produced and handled to the same standard as the police handle normal computer seizures, which is generally extremely good. That was lost before the courts, but the proposition that was endorsed by a judge in an unreported judgment and that came to be adopted was that there should be a golden or certified copy of original data as it was obtained by the service provider and supplied to the police, and it would be retained in the custody of the communications service provider. Now, that was used as a phrase for standard practice, but was never understood, and for many years, although I think it has ceased now, the SPOCs would deal with this by sending back their email to the communications service provider, and the communications service provider’s staff would send a statement back saying, “We recognise this as being the kind of data we use in our company,” and think that was good enough. So we have already seen those kinds of problems in the way that the SPOCs worked in the first decade.
Q758 Lord Strasburger: That was quite a long answer to a short question. Could I just try to distil that back and see if I have understood you correctly? You seem to be saying that, because the authorities are unwilling to disclose the mechanism behind the filter, it is not possible to validate the effectiveness of the filter and it is not possible, therefore, to put the evidence that falls out of it before the court in any meaningful way. Is that right?

Duncan Campbell: I believe they would not produce it in the first place, because they would foresee the issue of technical difficulties.

Q759 The Chairman: So whatever other use the Security Service or the police could make of a filter, using it as evidence in court is unlikely to be one of its main functions.

Duncan Campbell: On the basis of as much information as we have as to how it would work, which is, of course, little, that is my view.

Q760 Lord Faulks: I have just one thing; perhaps you can help me, Mr Campbell. We have a letter from the Director of Public Prosecutions suggesting that some of this evidence previously has been admissible as business records hearsay. In your capacity as an expert witness, are you familiar with this concept?

Duncan Campbell: Yes, and what he says is correct.

Q761 Michael Ellis: Of course, it is right, is it not, Mr Campbell, that very complicated evidence, including of a forensic nature, perhaps cell-site analysis, is already produced in court on a regular basis. It does not seem to hamstring the courts in producing relevant and admissible evidence of a modern type. They can handle it, can they not?

Duncan Campbell: The use of cell-site evidence has become increasingly established over the last 15 or 16 years. It has a degree of technical complexity to it. It is generally reduced to maps and put in a form that is helpful.

Q762 Michael Ellis: Yes, and so with cell-site analysis, which is the location of mobile telephones, usually the parties in court would stipulate or agree between themselves that the evidence has been obtained in a certain way and make an admission to that effect, so that the jury were not troubled with unnecessary complexities.

Duncan Campbell: The courts always admire a situation in which experts for the two parties seek to agree as much as possible and then precisely distil down that on which there is disagreement and on which the jury should deliberate.

Q763 Michael Ellis: That could happen in the instant case, could it not? It would not need to necessarily be explained to the jury in finite detail how everything happened. How scientists obtain DNA from a sample of blood would not necessarily have to be explained, but merely the bare fact that the scientists have come to the conclusion that the DNA within blood is that of the suspect.

Duncan Campbell: It is axiomatic that if the experts advising each side agree, then there is only a single joint statement to come before the court, which the judge would normally accept. I think I gave perhaps an over-detailed answer to Lord Strasburger, but in the area where the filter comes through—and I speak from a shared ignorance of what this filter will really be
Q764 Michael Ellis: If I can just take a step back, do you accept the premise that there has to be a legal means for interception of, in this case, data communications? Do you accept that to defeat the ends of terrorism, serious criminality, paedophilia and the like there has to be a means to do that?

Henry Porter: Yes, I do, but I believe in targeting the people that you propose to prosecute—the people you believe to be criminals. I do not believe that this entire nation should subject itself to a massive surveillance campaign by a few people who appear to be unscrutinised, their methods untransparent. But I certainly think that we should have these powers and we do have these powers.

Q765 Michael Ellis: Yes, and have had them for many years.

Henry Porter: Absolutely, no contest, and there are, what, half a million of the interceptions now per annum, roughly?

Q766 Michael Ellis: Of course, we should emphasise that this Bill does not deal with the interception, as such, of content. This is a different matter. This is not something that is seeking to read people's emails, which has been an aspect of the misreporting that I am sure you would all agree has taken place.

Henry Porter: Can I disagree with that?

Q767 Michael Ellis: You disagree with what?

Henry Porter: Yes, of course, the Bill lays out the difference between content and the data of the communication, but the fact of the matter is we all know in this room that the data surrounding a communication is as useful and can lead you to the content of that communication, and so the difference is very much a spurious one.

Paul Heritage-Redpath: If I could address the point, going back to DNA, ultimately with DNA you have a physical sample. You may disagree on how the analysis has been done, but you have something that is repeatable. With digital evidence, unless you have an audit trail of how it came to be all the way through, there is the possibility that somewhere along that way somebody may have tampered with it.

Q768 Michael Ellis: Yes, but Mr Heritage-Redpath, you need the audit trail as well with DNA or other forms of evidence. You need to be able to say that blood came from X person. You could not just magic up the sample and say it matches the defendant.

Paul Heritage-Redpath: Quite, but what I am saying is that in the case of all normal evidence, the police force, who have done a splendid job for many years, have targeted it in a particular case. What we are talking about here is something entirely different. We are talking about, let
us say, on the face of the Bill for the moment, capturing data about all communications lest it might be necessary or helpful at some point over the next rolling 12 months. That is a different thing to a targeted investigation.

Q769 Michael Ellis: But you accept, do you, that there needs to be a legal means for police and law enforcement agencies to lawfully go about this type of activity? You accept that fundamental premise.
Paul Heritage-Redpath: I do, and I think the way the Home Office have sold this Bill is that everybody accepts the fundamental premise that we should have the means to combat criminals, but it is not then a stage to say, “Having accepted that, just sign this Bill off,” because those are two different things.

Q770 Michael Ellis: Do you and your colleagues also accept, if you accept that premise, that the legal means have to keep up with modern and novel methods of communication? So, if it is lawful and has been for decades to intercept, for example, landline telephones, do you accept that modern methods of communication cannot be simply ignored, because criminals will use those modern methods of communication to defeat the aims of justice?
Duncan Campbell: There was a time, of course, when there was no law on interception of communications. We, the press—I and the press in large measure—pushed that into happening, and I do take pride in that.
Michael Ellis: Congratulations.
Duncan Campbell: Thank you. I hope it was sincerely meant.
Michael Ellis: It is. I try to say everything sincerely, Mr Campbell.
Duncan Campbell: I completely agree with what you say, of course. It is fit, proper and necessary that interception of communications and processing of communications data be available as part of the armoury to combat all the things you have mentioned. That is not my problem with this Bill. My problem is that it is not fit for purpose. It has not been thought through and it is not going to work. Leaving aside human rights, we are required to test issues like proportionality and necessity, and, in this forum, we are also required to test value for money and technical efficacy. Now, the witnesses who came here on the first day said to you, “We will spend all this money, and by 2018 one in six, 15%, of communications that we would like to get we will have no data about.” Now, that is a huge amount of gap that is, on their own evidence, not going to be remedied. Where that data came from, we do not know—whatever survey assessment it is—but that simply raises the question of whether it is even achievable and, of course, it is not achievable to get everything. Our police forces and our security services are doing the best jobs they can. They are going to get it wrong sometimes. There are going to be some dark areas.

Q771 Michael Ellis: We cannot catch every burglar, can we?
Duncan Campbell: Right. So once you have accepted, as I accept, your premise, as I must, you must also, with respect, accept the other premise that there will always be the dark areas and that, therefore, the proper area for debate is fitness or proportionality, necessity—necessity given the other types of data that can be used in investigations—technical effectiveness—can it work—and cost efficiency. Then come all the human rights criteria—the fact that you do terrify people by creating powerful laws.
Q772 **Michael Ellis:** On the technical efficiency aspect and the other aspects that you mention, therefore, you do not think the Bill is strong enough.

**Duncan Campbell:** No. I do not think the Bill is capable of getting to 100%.

Q773 **Michael Ellis:** But nothing can get to 100%, can it, in all seriousness?

**Duncan Campbell:** Exactly. Exactly.

Q774 **Michael Ellis:** We cannot arrest 100% of burglars, even with fingerprint technology. We cannot do that, so we can do the best that we can do. Gentlemen, on this point, which is the necessary and proportionate aspect, the Bill envisages that any request for comms data would be necessary and proportionate. It is a safeguard written into the Bill and that would be verified by a senior officer. Now, we have, and have had for many years, aspects of our civil liberties that are affected by the opinion of senior officers. So, for example, within the 1984 Police and Criminal Evidence Act, a superintendent has the right to extend detention before anyone is charged in a police station. A chief inspector can oversee ID parades and the like. So there is a safeguard there that we are used to in the English criminal justice system. So do you not envisage that those safeguards can apply equally well here and, if not, why are you worried that they will not work here when they have worked for decades elsewhere?

**Henry Porter:** I hate this idea of self-authorising this sort of power to one individual. One individual may act in one way, another one may act inappropriately, but what I want to see is scrutiny. I want to see how this process happens, and I personally think it should be in the public domain—these authorisations should take place in public. After all, we are talking about a democracy that is a fragile democracy. If you look at what has happened over the last 10, 15 years, we had an ANPR system pushed through the country, cameras recording registration numbers everywhere, on every motorway and through every town centre. This happened without even Parliament granting the money. It happened because ACPO decided that it should. You have CCTV cameras being enabled very gradually with face recognition technology. You have CCTV cameras in schools, in cabs, in trains, in pubs, in restaurants. What I am saying is that this is part of a very, very serious move towards what could easily become the structure for a police state.

So let us just go back to the authorisation. The police are not perfect. They have misused ANPR information to track legitimate protestors. There have been occasions revealed during the Leveson Inquiry where police officers have accepted money to give journalists information, to say nothing of the misuse of the Police National Computer. I just do not think this power should be just given to the police, so I am not as happy or as content as you are about the way that might happen.

Q775 **Michael Ellis:** We need to move on. Forgive me. Are there any brief comments anybody else wants to make on that?

**Duncan Campbell:** In response to your question about senior officers signing on necessity and proportionality, that is necessary but it may not always be sufficient. I think, and some witnesses have put forward, that a much better scheme would be a multi-level surveillance authorisation, which, to some extent, already exists in terms of intrusive surveillance. That should be applied to the communications data schema, so that you have a signing off at higher
levels or a warrant from sufficient authority, depending on the degree of intrusion involved. But these are the appropriate and necessary processes.

Just two minor points: although it was not required by law, the police sensibly adopted a scheme whereby assistant chief constables would be required to sign off on location data requests. They have dropped that now, but they saw the degree of intrusion necessary and they said, “A chief superintendent is not enough; we will go to ACPO rank.”

The other point I would make is that the European Court has required that the procedures for examining, using and storing gathered communications material should be in a form that is open to public scrutiny and knowledge, and along with authority that is an important part of the process.

Q776 Mr Brown: I am quite interested in moving this on to the point about safeguards. As you have rightly pointed out to us, this is a framework Bill, and once the framework is agreed as primary legislation the flesh on the bones will come as secondary legislation. The opportunities for Parliament to say “no” or “pause” or “think again” are strictly limited, so it is important to us that we get this right. I am interested in what sort of safeguards we would insist are included. We have given some thought collectively amongst ourselves, Mr Campbell, to the point you referred to about a multi-layered authorisation scheme. It is there now, but would it be possible to extend that? In particular, I wonder if you could say to us what your thoughts are on the idea of a judicial element to the proposal. Should the magistrate’s warrant that is proposed for local authorities be extended? Is it the right idea? Is the specialist authorising officer a better or a weaker safeguard than a magistrate who is independent but might not be as well informed or as experienced, or might be in awe of the police?

Duncan Campbell: They all get it right much of the time and wrong some of the time. I think a multi-level review of this whole area would be very sensible, and taken within that would be escalating ranks within the police force or security or intelligence services through to stepping outside to magistrates, district judges, judges, as might be appropriate to the degree of surveillance. The situation is that this business of content versus communications data is a shibboleth from the 1980s, when we had a plain old telephone service and clunky things called printometers, which could occasionally be attached to lines. Now, without going into the disparate technology of it, I think witnesses have told the Committee that the internet comes in layers, that the first layer is communication, but the content contains communications data about the next layer, and that content, in turn, contains communications. It all dissolves when you look at some of the very complex things that operate on the internet, and it would be quite appropriate just to review how distinct content and communications data really are, as part of an overarching review.

I know there has been a well tested argument about bringing intercept data into the courts. I have seen it. I have worked on it when it comes from overseas jurisdictions, and it is very hard to understand the degree of resistance, except a sort of primal fear of letting the adversaries know that we cannot do some things. So you could really quite usefully do an overarching surveillance scheme with officers of different ranks, judges of different authorities, and a surveillance commission that would act as the check and balance on whether the wide remits on all fronts had been followed.
Q777 **The Chairman:** That term “surveillance commission”, you see that as a separate body and not a slightly enhanced role for the Interception of Communications Commissioner? Do you see him having any role in that?

**Duncan Campbell:** I think debates here and elsewhere have pointed to a need to really enlarge the scope and, indeed, independence of the Commissioner or whatever might be the successor body.

Q778 **Mr Brown:** I would like to elaborate on this. How far is a separate magistrate a safeguard and is there any further safeguard to be gained in restricting the number of authorities? The Bill only applies to the police, the security services and so on, although it is clearly shaped in such a way as to allow other authorities to be added in later and, indeed, there are hints as to which authorities, including local authorities, the Gambling Commission and so on, will be added in later. Do you think there is any safeguard to the public in restricting the authorities that should be added into the Bill?

**Henry Porter:** I certainly do, because if you look at the way RIPA was abused in the first half of the last decade, you had punt operators in Cambridge, a woman who applied to a school in Poole, Dorset, for her kid and was thought to live outside the catchment area, and I think you even had eel fishermen in Poole Harbour being subject to a major surveillance operation. So there is a predilection for abuse. We are not a naturally democratic country sometimes, and people will use these opportunities to use their power in an unpleasant way.

Q779 **Mr Brown:** A disproportionate way is what you are saying to us.

**Henry Porter:** Yes, I, indeed, was going to say that. So yes, I do think we should restrict as much as possible the number of authorities, and I think the maximum amount of transparency in the process that goes to authorisation is absolutely vital. One of the problems with this Bill is that it is not very specific. Duncan has been very eloquent in saying we do not really know what we are talking about, because it is non-specific in so many areas.

**Paul Heritage-Redpath:** Being in trade, I am required to make a business case for any investment that we do, and if I made a business case like this I would be sacked, because we have not been clear about what it is we are trying to achieve, how much it will cost or how to do it. The justification on the face of the Notes, as Michael put it, was, “This is all about catching criminals.” Now, that narrows down what you are doing, but you get to the end of the Bill and it says, “Oh, and by the way, here is a list of X hundred authorities who might be interested.” So in terms of proportionality, if it were just crime we would be having a much more targeted and productive discussion.

**Henry Porter:** Can I make one point about crime? Crime is on a steady downward trend. Whatever the economic circumstances of this country, steady, steady, steady, it goes down. For the last 20 years I think it is down 27%, the last 12 months 6%, and yet we are constantly being told by politicians that we have to guard ourselves against this terrifying society we live in. One of the main planks of this Bill is to fight crime, but let us just look at what is happening out there: we are a very law-abiding society and we are getting more law-abiding.

Q780 **Mr Brown:** What the public—our constituents as well as your readers—are worried about is that something they have done—on the internet or some communication, some bit of their private life they do not want their friends and neighbours to know about—is going to be
discovered by a snooper and exposed in some way. How best could we safeguard against that? These are innocent people who are entitled to their privacy. How should we ensure they get it?

**Henry Porter:** Well, let us not have a vast database with large amounts of information in it. That is one way of guarding people’s privacy. The second way is not to collect that information in the first place. I have a great problem with the argument that, because people give so much away about themselves on social network sites or to Tesco or to whoever, the Government and the state have a right, therefore, to take all that information and put it into a database. If you listen to Ross Anderson, the professor you had give evidence earlier this year, he would tell you that there is no way that you can have a database that is, at the same time, large, secure and functional. That means that, once your constituents’ information is in a big database, it becomes much, much more vulnerable. So my answer is: do not have this Bill. It is very simple. Mr Ellis has made very good points about targeting criminals, but to collect this massive amount of information on people means that one day it will become vulnerable, maybe to a journalist at News International or a detective working for News International. This is the point: once you have these databases, they are a treasure chest.

**Duncan Campbell:** If there is an obvious concern, indeed, in auditing SPOC data down the years, I have always had it in mind to watch for an extra one being slipped in to bung to a journalist. I have not found any, but it may be that Lord Leveson and the associated police inquiries will be leading to this in due course.

Mr Brown’s point about the sensitivity of data and the risk it could leak would, in my view, flow largely from creating this database in advance or these databases that are required. Again, rather than the obscurantism of the Home Office approach, we can address this quite specifically in the case of weblogs. In my expert capacity, I have to sometimes look at weblogs that, when seized from computers, can sometimes go back years and years and, frankly, they terrify me. The intimacy with which you can see what somebody is doing, what somebody is thinking, you can infer when their attention has strayed from their partner to some other prospective sexual target—it is written there to be seen. Now, if that person is under that degree of surveillance, because their device has been seized by the police because of a suspicion, then you can at least see how that comes about, and the rest of the population can be reassured that is never going to come to pass unless officers do come through their door for whatever reason. If you move to what was envisaged under RIPA and which will be reconstructed here, then, at the very least, the big internet service providers are going to be asked to store that kind of data, although we have no clue as to the depth of knowledge, and that degree of intimacy. That means that, if anyone wants to go on a trawl, whether authorised or unauthorised, whether the purpose might be approved or not, they can trawl to see who has been accessing special clinics. They can trawl for who has been going to particular websites. They can trawl to draw up profiles and demographics just in the same way as Google does. Clearly, most or all of that would not be proportionate. How do you stop it? Do not do it in the first place. Stick to what you get on people’s computers.

**Q781 Dr Huppert:** I am very much enjoying the comments you have made so far. It has been a great pleasure to listen to. Can I look at some of the issues to do with parliamentary scrutiny and what is envisaged within this Bill? You have all expressed concerns about the, I guess, skeletal nature of the Draft Bill, for example, clause 1, which, to paraphrase slightly, says
the Secretary of State can, by order, do anything she likes. Do you think that is inappropriate, in that there will be a system where you have this primary legislation, there is then an order, which is essentially unfettered, and that provides then for notices, which nobody gets to see? Does that seem like an appropriate way to take things forward?

*Henry Porter:* It seems mad for a democracy to even be considering this behaviour. I am amazed we are in this room countenancing this legislation. We have all brought ourselves to a point where we feel it is necessary to think in these terms, but step back and imagine what Wilkes would have said or any of the other great men who have been responsible for fighting for this democracy and the liberal, free society that we have. Imagine Wilkes listening to you now and saying, “Well, these notices will be shuffled past, nobody will take any notice of them.” It is unimaginable that we are even considering this.

In the last Government, I used to go to Select Committees to watch one or two of the Bills being discussed. I was astonished that we were even thinking of this way. There was a thing called the Legislative and Regulatory Reform Act, or some mad scheme.


*Henry Porter:* That was it. Sometimes—when you just said that—I think how can we countenance this? We must be thinking of our democracy in different terms from the ones I was brought up with. We have to sit on this Bill. I do not care what party anyone comes from. This Bill is dangerous. This Bill is really, really dangerous, and if we let it get through in its current vague terms and then things are just added on, and nobody pays any attention, we will not have a democracy.

*Paul Heritage-Redpath:* We are all responsible for public money, at the end of the day, as well. I was involved in the e-conveyancing scheme with the Land Registry. This was a scheme where industry was consulted and where the people who were involved were very clear about what they wanted to achieve. There were very tight, small, objectives. It was £11 million of public money and it never came to fruition. I do not know anybody in the industry who thinks this scheme can possibly work and, to use a layman’s analogy, I think we talked about telephones before and in his last piece Duncan mentioned weblogs. To be very clear, Duncan meant, I think, just the record of the URL that somebody had gone to—not content, just communications data. Now, the way the internet works and the way ISPs work is we try to move information around as fast as possible. The last thing we want to do is look at it. To try to explain how difficult this would be, what we do is akin to a traffic policeman going, “This way, that way.” The original scheme, the old scheme of the great centralised database, started off by saying: “That traffic policeman will say, ‘Stop, each car; I am going to ask the address you are going to and jot it down.’” You can see that will not fly. So the new improved scheme is to say, “Well, okay, we will just channel all of the internet and keep it. While it is going past, we will just keep it for a year on a rolling basis.” Again, it is just common sense: how is it possible to get the capacity to do that, even if you agree that is a good thing to do? It is just like trying to pick the M25 up and photocopy it as it is going past. You cannot do it.

*Duncan Campbell:* That is a concern with the filter. There is no detail, as ever. We start from ignorance, but it is, to my mind, inconceivable that the tasks anticipated for any filter could be done on data as it streams past. Therefore, what you are left with is the elephant in the room that surrounds this Bill, which is we must not call it a national database because that is what the last Government did. Therefore, database is avoided, but in fact database is essential.
I fear the Home Secretary has not been well served by her officials on this. One is not privy to what goes on, but the sense is, “Do not worry about this; it is all techie stuff you really do not need to know. Parliament does not need to bother its head. It is the big complex internet; we will sort it out.” Even if it was not this very sensitive and important area of legislation, what you look at with any knowledge of large public sector IT projects is massive expenditure, billions of pounds, on a future that is untested and on technology that seems incapable of being specified and that has not been described to the people whose equipment it will attach to. Let aside all of our other worries, the total gap in the information about how this will work means that there must be a very high probability that this will become yet the latest public sector, massive, cost-overrun IT boondoggle.

**The Chairman:** We need to conclude. Move on to the last question, please.

**Q782 Dr Huppert:** The officials will have a chance to speak. They are coming back to this Committee, and it is certainly a frustration of mine that we have not seen the draft of the Order at all. The Home Office position, if I try to paraphrase it, for making it so broad is that there is a fast pace of technological change and they want to have a Bill that is future-proof. I think that is the position. Given that we do believe that there is a legitimate role for communications data, how would you structure something so that you could resolve this? Would you have a series of Bills with sunset clauses? Would you have legislation that was extremely precise and needed replacing on a regular basis? What do you think would be the most sensible and practical way of getting the benefits of communications data without the harms?

**Henry Porter:** First of all, I think if you are going to give this power to the police and the Security Service, you have to have a period when you say, “Is it working? Is the scrutiny working? What effect is it having on our society? Is it having a chill on our internet and web industries? Is it having a chill on journalism?” So definitely you need to review it. If this is going to go through, you definitely have to have a sunset clause or some moment when you say, “How has this affected us?” Let us not just let it drift into the future imagining that it is working all the time as we planned originally.

**Duncan Campbell:** I think this Bill is future-proof, but in the worst possible way. It is future-proof in the sense that the Home Secretary seeks to have the power to her and her successors, in the words of the Bill, to do anything they like once the universal surveillance engine is connected up to the entire national internet. So, for that reason, it is additionally terrifying. The alternative would be to reset the mechanisms of surveillance and allow that there would need to be fluidity as new data sources came along. A surveillance commission, if that were to be recommended, with access to both human rights advocates and technical experts as well as senior judicial figures, could address that—and with as much transparency as possible, which is the opposite of where we are now. And it will not be Twitter that we will be talking about in six years’ time, it will be something completely new that no one has thought of now. So I do not think you can put in place a good future-proof Bill, but you could put in a transparent, thoughtful, representative system of reviewing how you adapt access to intercept and communications data as the technology changes.

**Q783 The Chairman:** Mr Redpath, anything to add, finally?

**Paul Heritage-Redpath:** No, that is perfectly fine, thank you.
The Chairman: In that case, thank you very much. We have overrun our intended time. That is because of the interest all panel members had in hearing your point of view. You spoke with knowledge, authority and passion, and thank you very much for giving evidence today.

Crown Prosecution Service (QQ 784-839)

Examination of Witness

Witness: Keir Starmer QC, Director of Public Prosecutions, examined.

Q784 The Chairman: Welcome, Mr Starmer. I am sorry we have kept you waiting. I know you are on a tight schedule today and I am sure we are so grateful to have you here.

Keir Starmer: I do not think you have kept me waiting, so I am very grateful.

Q785 The Chairman: I am sure colleagues will also respect the tight schedule you are on and we will be as crisp as we possibly can. Now, although we know who you are, for the public record, sir, I would be grateful if you would just state who you are and what you do.

Keir Starmer: Yes. Keir Starmer, Director of Public Prosecutions.

Q786 Michael Ellis: Good afternoon, Mr Starmer. Just to start off this session with you, do you consider that this Draft Bill, which no doubt you have had an opportunity to study, in its present form would allow your organisation or the Crown Prosecution Service to present evidence in court, where it existed, that would enable prosecution functions to be carried out? In other words, would it work?

Keir Starmer: Yes, I think it would. We use communications data at the moment routinely and it would allow us to continue to do so.

Q787 Michael Ellis: You probably were not present in the room, but we have heard other witnesses say that, in their view, it simply is technically not going to be something that would work; the courts would reject it. But you say that already communications data is in use and you do not envisage problems with admissibility or relevance of evidence.

Keir Starmer: Communications data is in use routinely. From a prosecution point of view, what it establishes in many cases is, if you like, the chronology of a crime, proof of association, links between individuals. Linked with other techniques it can establish presence at a particular place at a particular time and corroborate witnesses, etc. We use it routinely at the moment in a wide range of offences. Admissibility has not been a problem in the past. Usually the data is admissible, either as real evidence or as hearsay evidence under the various statutes and criminal procedure rules. I do not anticipate that is going to be a particular problem going forward.

Q788 Michael Ellis: Do you equate it, possibly, with another example that I used earlier, cell-site analysis of mobile telephone locations or DNA, in that you would not necessarily need to
explain to a jury exactly how it is that scientists are able to extract DNA from a blood sample, but you would have to satisfy a jury that the blood sample was obtained legitimately, that its provenance was accurate and that a responsible scientific officer had performed his or her calculations correctly? Admissions can be made between the prosecution and defence to that effect, and are, in most cases, where DNA or other technical or forensic evidence is adduced. **Keir Starmer:** I do not think explaining it to the jury is a particular difficulty, because once this is adduced, either as real evidence or business records, it is not very often in dispute. It is simply what it shows us that is relevant, and what we would very often do is use techniques to establish for the jury X was talking to Y at this particular time when, let us say, a consignment of drugs came in, and X, Y and Z were all talking together. We say they are the conspirators and, linked with cell-site analysis, we can probably say, “And they were standing in the following places when they were having the conversation.” Presenting that to the jury is not particularly problematic, because the basic facts are agreed and it is what you can read into it that becomes the issue. Very rarely is it disputed that X was talking to Y or where they were. It is the explanation that is given for that behaviour that becomes the issue for the jury. So I am not saying that presentation is never an issue, but it is not usually an issue.

**Q789 Michael Ellis:** So this Bill deals with not the content of material but the provenance of it, where it has come from, where it is going to, the time, the date stamp, that sort of thing. **Keir Starmer:** Yes.

**Q790 Michael Ellis:** Therefore, it can apply, to use another example, to obscene images, for example in a paedophilia case. Where that has been transmitted over the internet, one of the mischiefs that this Bill would seek to redress would be that it would be possible to ascertain internet addresses and date and time stamps and so on. Is that correct? **Keir Starmer:** Any offence that we prosecute that involves the internet in any capacity usually requires us to produce communications data to show who it was that was accessing what part of the internet at any given time, and it can run through a range of offences. One example we have on a schedule here is a harassment case, establishing who it was that sent various messages at various times.

**Q791 David Wright:** The point here, though, is that much of that evidence at the moment, Mr Starmer, would be obtained by seizing a person’s hardware—entering their property, taking their computer away, analysing what they have been doing with it. It would not be about tracing material that is going across the internet live, if you like. It is about seizing equipment. **Keir Starmer:** It is a bit of both. A lot of it is seizing equipment, but not all of it. From our point of view, we are obviously concerned with the product and what we can establish from the product.

**Q792 Michael Ellis:** In a nutshell, Mr Starmer, would this Draft Bill, as envisaged, assist you and your agents and officers in the exercise of prosecutions of serious offences in this country? **Keir Starmer:** Yes.
Q793 Lord Strasburger: I think we are starting to get confused on this Committee between the benefits that law enforcement agencies and prosecutors are getting from the existing legislation—RIPA—and what additional benefits they might derive from this Bill, if it were enacted. I am hearing from what you are saying that you are, at the moment, talking about the benefits you get from RIPA.

Keir Starmer: Yes. I am talking about that. That is what we have experience of and our concern is that we should maintain that coverage. I do not doubt or challenge that there is a privacy aspect here and there is a balancing exercise. I understand that, and Parliament has to think about that carefully. All I can say is from a prosecution point of view communications data is extremely useful in many prosecutions, for the obvious reason that it allows us to establish who spoke to who when, quite often where they might have been at the time and patterns of behaviour. If you are trying to prove a criminal case, that is extremely useful information.

Q794 Lord Strasburger: That is based on the existing legislation.

Keir Starmer: Yes.

Q795 Lord Strasburger: On the issue of admissibility of data, the question that we will be driving at shortly is how, under this Bill, evidence that is derived through the filtering process would stand up in court. But I think we are going to come back to that later on.

Keir Starmer: By all means.

Q796 Mr Brown: The public are frightened that data held on them by various Government agencies is accessible by corrupt public servants, and sold on to somebody with no right to have it, but who wants it for purposes of their own; the topical example is journalists but it does not have to be that. As I understand it, the offence committed by, say, a corrupt police officer in taking information from the Police National Computer to see whether someone had a criminal record or not is misconduct in public office. How easy is it to prosecute the offence of misconduct in public office and how frequently is it prosecuted?

Keir Starmer: Misconduct in public office is a common law offence with fairly straightforward elements. It has to be misconduct that reaches a certain threshold in order to render it criminal. That would be one offence that could be used. There would be others, I suspect: the Data Protection Act and Computer Misuse Act, possibly offences under RIPA itself. I am not sure we would have the figures under misconduct, and I am not sure they would tell the Committee very much if we were able to produce them, because, I suspect, that where there have been cases involving misuse of data, it is probably a number of different offences that we have considered in individual cases.

Q797 Mr Brown: Do you believe the present law and the practicalities of prosecuting it adequately protects the public from the commissioning of this offence?

Keir Starmer: I think the Computer Misuse Act was strengthened a number of years ago and, to my knowledge, it has not caused us any great difficulties. That is from my memory. I am very happy to come back if it would help the Committee on this, but so far as I am aware, we have not run into any particular problems. If someone has misused data, we have not found ourselves unable to prosecute for want of a relevant offence, so far as I can remember.
Q798 Mr Brown: Could you have a think about it and come back to the Committee?

Keir Starmer: Certainly.

Q799 Craig Whittaker: Just very quickly, I just seem to get to grips with what is going on in the various avenues of this Bill and then I get blown away. You said that you often use live data communications from the internet as well as historical stuff from hard drives and stuff; I think that is what you said earlier on. How many cases would you say do not come to prosecution because you do not have the ability to get to the stuff that is in this Bill?

Keir Starmer: I am afraid I cannot give you an answer to that question. I apologise. The reason is that if there is not the evidence, then it is unlikely the case would ever be presented to us. We are presented with cases that the police have investigated and, therefore, they present a file where they think there is enough evidence. Now, there may be cases where we would say it would have been jolly helpful to have had a bit more of this or a bit more of that, but we do not normally have a case where I would be able to say, “If you had had that, we would have been able to prosecute,” and we do not record that. There may be some cases. I am not saying that would never happen, but we would not then record it as a case that, as it were, we could not take forward because there was a gap in this particular piece of legislation.

Q800 Craig Whittaker: Just very briefly, could I ask for a best-case guesstimate from you then as to how much extra information this Bill is going to give you that you physically do not have now under current legislation?

Keir Starmer: I think our primary concern is to ensure that we can continue to use the data that is currently available to us, and the concern is that it is retained and used in a particular way at the moment. If that changes in the future—and I think the evidence on this has come from the Home Office rather than us—we want to maintain the capability that we have. From our point of view, it is a reasonably simple approach. The more people use communications and the internet to transact business and to commit crime, the more important it is for us to be able to use evidence to establish that they have done so, either when it is an offence that involves the internet itself, and we have some of those, or where it shows elements of agreement, conspiracy, for other offences. So that is our concern.

Q801 Michael Ellis: So, because you are prosecutors and lawyers, you would not necessarily know; it would be the police who would know that they cannot obtain evidence against a member of a gang, for example, because they cannot achieve that evidence. You would only know or your people would only know whether they can prosecute files that are laid before them by the police.

Keir Starmer: Broadly speaking. The police would put the file before us. Now, in big and complicated cases there is a conversation that goes on, and we encourage it, where the police may bring a file that has nearly enough evidence but not quite enough, and we might suggest lines of inquiry to them, but they would then carry that out. I can envisage in the course of that discussion it might come up that they would have liked to have got X but could not get it.

Q802 Michael Ellis: Yes, and further to my colleague Mr Brown’s question about penalties for improper use, would the offence of perverting the course of public justice possibly apply in
some cases if there was misuse in the obtaining of communications data? Could you see circumstances in which it might apply? That is an offence for which there is no limit to the amount of penalty, is there? Life sentences are applicable.

**Keir Starmer:** It might apply. It is not entirely straightforward. I certainly can conceive of some cases that might fall into the category of perverting the course of justice. I am not sure it would be the starting point in most of these cases, but it might be available.

**Q803 Michael Ellis:** Finally from me, would you say that there has been misinformation about this Bill in the media? You may not be able to answer the question. I do not know how closely you have been following it in the press, but would you say there has been misunderstanding or misinformation about it?

**Keir Starmer:** I am not sure I am in a position to comment on that. I have been following it, probably not as closely as everybody else, but I have been following, just at the moment, quite a lot of things going on in the media. So I think I am not particularly well placed to give a sensible answer to the Committee on that, I am afraid.

**Q804 The Chairman:** Mr Starmer, could you help me out here? I have heard you say probably a couple of times today what you are basically interested in is who spoke to who, when and maybe where they were with the tracking information. That seems to me to be fairly basic stuff, and I do not think any of our witnesses, including those, possibly, in the last panel, who were quite critical of the Bill, objected to that basic stuff being used by the police or accessed—who spoke to who, what, where and when. But the criticism of the Bill is that clause 1 seems to include a huge range of additional material, and logging on to internet addresses and so on, which could give a lot more information than who, what, where and when. Is it your view that you need all this extra stuff, or do you basically want to ensure that, whatever Bill we have in the future, you are getting the basic data you seem to be using at the moment—who, what, where and when?

**Keir Starmer:** First and foremost, we want no reduction in the data that is currently available to us. If it is right that those producing the data may not need to do so or retain it in the future in the way they have done in the past, and that is going to impact on our ability to get that data, then that is a concern. There are some offences where what we need and what we have had access to in the past has gone beyond that. We had one case called Dark Market, which was about, as the name suggests, a covert market where you could trade in stolen goods, cloned cards, etc. To prove that case we needed to have a lot more information about who was doing what on a particular website. So there is a category of offence—website-based offences—where we need to go beyond that, but our first concern is to ensure there is no diminution in the sort of evidence that is currently available to us and is used for pretty obvious reasons when you consider what it can show.

**Q805 Lord Jones:** What is your experience of the extent to which internet communications data is currently adduced as evidence? Is this evidence relatively easy to explain to a jury? Do you have some views you can give us again? Juries, I think, generally are not very expert.

**Keir Starmer:** I was alerted to the fact that there would be questions about volume and numbers. I am afraid that we do not track, on our own databases, the cases where we have used particular types of evidence; therefore I am not able to give an answer. We have given in
our written evidence some examples of the types of cases. Communications data itself is used routinely. So far as internet communications data is concerned, I am not aware of any case where it has been overly difficult to present it to the jury. Presentation is not a particular problem for us, because once we have it in admissible form, frankly, most of the time the fact of it is admitted, and therefore it is simply for the prosecution and the defence to explain, as best they can, what they read into the information.

**Q806 Lord Jones:** Juries are a very British thing. Are you able, just for our benefit, to try and get into the minds of the many juries that sit throughout the nation every day?

**Keir Starmer:** No, I am not. I am no better equipped to answer that than anyone else is under the current regime. What we do though, just perhaps to give this some context, is where big cases fail I will very often have a case review panel, and walk through with the team—sometimes our team, very often our team and the police—the decision-making and ask ourselves why we think it failed and what we would do differently. As far as I can remember, I have not come across a problem where we thought it was because of the presentation of internet data communications that we have hit a problem. However, by its very nature, that is a selective exercise.

**Q807 Lord Jones:** Generally speaking, do you retain faith in the jury system?

**Keir Starmer:** Yes.

**Q808 Dr Huppert:** Mr Starmer, first, can I just ask when were you consulted on this Bill? When did you see what it said, and have a chance to talk to the Home Office about what implications it would have for your work?

**Keir Starmer:** Some months ago. I do not know the precise date, but I am more than happy to share with the Committee the dates on which we were asked to provide comments.

**Q809 Dr Huppert:** I think that would be very helpful to have a look at. Can I then ask about the admissibility of some of this, and the evidential integrity? I was struck by my colleague Mr Ellis’s comparison with DNA. My PhD was exactly on DNA and I am sure that you will be well aware of work by Frumkin and others that shows that DNA data can be faked, and this is why your predecessor decided not to take evidence that was entirely based on DNA. Presumably there are times when the accuracy of DNA evidence is questioned.

**Keir Starmer:** Yes.

**Q810 Dr Huppert:** So one would expect the same concerns with communications data, particularly if it gets more complex.

**Keir Starmer:** Yes.

**Q811 Dr Huppert:** Currently, we have relatively simple situations where most of the communications data that comes has been requested through a SPOC from a CSP presenting their own data, which they can be reasonably sure is accurate because it is their data they are passing on. This Bill envisages that a communications service provider in the UK would be using equipment that they were potentially supplied by the Home Office to collect data as it
transits through the network, that belongs to somebody else, is laid out in a way that they are not familiar with and is potentially encrypted in some way.

*Keir Starmer:* Yes.

**Q812 Dr Huppert:** Do you think that would raise questions in a court and that somebody would be able to ask, “Who can assure me that this is the data that was sent in the correct format?”

*Keir Starmer:* It might do, but I think the rules on real evidence and hearsay evidence have moved on quite considerably in recent years, and it has not presented us with a problem so far. That is not to say it will not, or there will not be challenges just around the corner; of course there will be. Historically, though, we have not run into those challenges and the courts have been a bit more robust about real evidence and hearsay evidence than they were in the past.

**Q813 Dr Huppert:** Who would be able to present the evidence?

*Keir Starmer:* With real evidence it presents itself. With hearsay evidence the rule now is that it can be produced pretty much as a business document without a witness having to adduce it. That is how it is done very often, and recently the Criminal Procedure Rules Committee has changed the rules to enable that to happen a lot more easily. So, as it were, the old approach for many years, where you would have to have a human witness who would faithfully sign a statement saying that this is how it was all recorded has been, to a large extent, substituted with a record that proves itself. Nobody knows what the challenge is going to be around the corner, but I can say that at the moment there is rarely challenge to that record.

**Q814 Dr Huppert:** But what I am suggesting is that that is because the record is currently a far simpler document. If I can move you even beyond that aspect of the Bill towards filtering, that means you would have a system where there is purely a black box, where no individual or organisation could be sure at all that there had not been something that had gone wrong, nobody would see the transitory data, and you would have the outcome of a search that could not be verified. So whether or not you have a person presenting it, no police officer—nobody—could be sure that it was correct.

*Keir Starmer:* We would have to work through the practical problems. I take the point that you are making. No doubt there will be challenges, and obviously, from our point of view, we would want to be sure that in any given case we could comply with our disclosure obligations and therefore we would need to have a level of assurance about how that process worked, because we do have those obligations.

**Q815 Dr Huppert:** Did the Home Office talk to you about how this might work from an evidential basis? Did they engage with you to make sure that what they produced was something that you could use, or are you now retrospectively having to try to work out how to cope with their phraseology?

*Keir Starmer:* The communications in detail they have had have been with my policy and strategy team and, with your permission, I will check with them what and when, so that I can present you with a full answer on that.
Q816 **David Wright:** Can I just press that a little further? So you have not had a briefing with the Home Office about how this filter arrangement would work.

**Keir Starmer:** Personally, no.

Q817 **David Wright:** How can you make a statement at the start of your evidence, then, to say you believe this Bill will deliver its objectives?

**Keir Starmer:** Because I have read the Bill and I understand how it is supposed to work, and I have read a good deal of surrounding material and briefings, and I have talked to my team in detail about it.

Q818 **David Wright:** Okay, and you believe that, even having not seen the detail on how the filtering arrangement would work and the way it would produce material and the kind of documentation it would produce, that would still be suitable.

**Keir Starmer:** I have looked at the draft, I have looked at the briefings, and I have looked at the background material. I have looked at the experience we have at the moment. There may be practical difficulties. There will, of course, be challenges, but I do not believe, on the basis of what I have read and discussed, that there would be difficulties in using this information in the future. If it is right that the capability under the current regimes will go down, that is something that concerns me.

Q819 **Lord Faulks:** Just picking up on that, Mr Starmer, I think it is fair to say what you are really saying is that there might be some challenges because of the width of the filter; the existing rules about business-records hearsay and the like might not initially cover it. At the moment, I do not think there is much issue usually with the admissibility of these records. There might be some initial challenge, but you would expect it to settle down in due course.

**Keir Starmer:** Yes. Of course there will be challenges. I would be surprised if there were not, but I have faith that these will be workable provisions.

Q820 **Lord Faulks:** The obligation of disclosure can be rather onerous. There is going to be a considerable amount of additional material. Do you envisage difficulties with, potentially, a sizeable amount of material that you might be asked or obliged to disclose, consistent with the Attorney-General’s guidelines?

**Keir Starmer:** I think we will have to carefully consider how we approach the disclosure exercise if this regime becomes law, and we will have to be careful to ensure that we are taking what steps we need to take to comply with our obligations, and that we are completely clear with the courts as to what we have seen and what we have asked for and what we possess. That can be achieved. We have achieved it across a number of different fields where there were obvious problems.

Q821 **Lord Faulks:** I appreciate the context in which you tend to see cases, but you have also told us that you will review cases afterwards. Have you been aware of this so-called data gap in the course of your work—the data gap that will potentially be filled by the obligation on CSPs to preserve data that they do not need for business purposes?

**Keir Starmer:** No, I do not think I can say I have seen that gap, but I am clear that the data that has been provided to us has been extremely useful and if it is right that what is now
retained may not need to be retained in the future and thus what is available will reduce, that is of concern to me.

Q822 Lord Faulks: Do you have much experience of the mutual legal assistance treaty process? We have heard it tends to be rather a slow process, but can you help us more than that?

Keir Starmer: It is useful, but it is a slow process. It is usually reserved for obtaining evidence after the commission of an offence where that evidence already exists in another jurisdiction. I think the difficulty here would be, first, ensuring evidence existed, because it had been preserved in some way, because no mutual legal assistance treaty helps if it has not been preserved; secondly, it is a rather slow process, usually measured in weeks or months and therefore, to my mind, it would not work well in this particular field.

Q823 Lord Faulks: There is one other point I would like to ask you about, if I may. We have heard from the Information Commissioner, who gave evidence to this Committee, about a tendency for police forces routinely to extract personal data from, for example, mobile phones of suspects and then retain that data even though that person is subsequently not charged. This may be a bit of an unfair question to field, but can you tell us, first of all, whether that is legal or not, under PACE or any other provision?

Keir Starmer: I am not sure, off the top of my head. I do not know. I can certainly work up an answer for the Committee, but it is not a straightforward question and it is not one that I have considered before. I am sure, if I have a shot at it, I will regret it in about half an hour when somebody gently points something out to me.

Lord Faulks: I apologise for asking.

Keir Starmer: On the other hand, I am more than happy, if it would be helpful to the Committee, to give a considered view in writing in a pithy way.

Q824 Mr Brown: That would help the Committee. You can see why we are interested in it.

Keir Starmer: I do, but I equally can see the trap that I am obviously about to walk into if I attempt it on my feet.

Q825 Mr Brown: I do understand that. Do you know if it is extensively done?

Keir Starmer: I do not know, but I do not think anything can be read into that one way or the other. I do not think I necessarily would know. I have not personally come across it, but then I see a limited number of our cases and I would not necessarily be privy to that if it happened. I have not come across it, but I really do not think anything could be read into that one way or the other.

Q826 The Chairman: If you could reflect upon the issue and let the Committee have a note that would be very helpful.

Keir Starmer: Of course.

Q827 Lord Armstrong of Ilminster: The Home Office are depending fairly crucially on the distinction between communications data and communications content, and content is dealt with not under this sort of Bill but under completely different arrangements. But the point
has been made to us in the course of evidence that that is a very blurred distinction, because what you can get now about data shades into content. If you know who has been speaking to who, when and where, and the frequency of conversations, you can get a long way towards content. Is this something that has concerned you or affected you?

Keir Starmer: I do understand why that point is made. A classic example here for us would be a case where we are able to say that a consignment of drugs came into port X at a particular time, and we think that three people were involved in the exercise. We look at the communications traffic between them and we establish that, by coincidence or, we would say, because they are conspirators, they were in contact throughout the passage of the drugs and when the drugs arrived they were in a lot of contact all of the time, and then it dropped off. Whilst we do not know the content of the conversations, we are often asking the jury to infer that they must have been talking about the consignment of drugs that have just been brought into the country. Now, that does not give the jury content, it does not allow us to rely on the content, but we are sometimes saying to the jury, “The only inference you can draw here is that at that time, as they were both—as we can tell using cell-site analysis—right there in the dock as the drugs came in, they were talking about the consignment of drugs.” That is a classic example of when we use that.

Q828 Lord Armstrong of Ilminster: I think you are really saying that that distinction retains validity for the purposes of this Bill.

Keir Starmer: The distinction does retain validity. Nothing here encroaches on content, but realistically and frankly speaking, we are, on occasion, inviting the jury to infer that A was talking to B about the crime that we are trying to prove.

Q829 Lord Armstrong of Ilminster: But there is a difference between inferring something from a series of events and listening or reading the content of the communication.

Keir Starmer: Absolutely, and a classic defence in that case would be, “No, I am the godfather of his child and we were discussing what I should get for its next present”.

Q830 Michael Ellis: Mr Starmer, just moving on a bit to the public authorities and who should access communications data, the Draft Bill limits those bodies that will have a right to use the powers provided to access communications data and all the other bodies will have to make a case to the Home Office as to why they should be included. Is that right?

Keir Starmer: I think that is right, yes.

Q831 Michael Ellis: So I was looking at the written evidence provided by the Crown Prosecution Service. Now, the Department for Work and Pensions is a Department that the CPS seems to wish to continue to have access to comms data, and this is clearly because of the work prosecuting benefit fraud.

Keir Starmer: Yes.

Q832 Michael Ellis: So how important is comms data to the work in the prosecution of benefit fraud for the DWP? Do you know?
Keir Starmer: Just by way of background, if I may, the DWP obviously investigate and prosecute benefit fraud. In March of this year, the prosecution function of the DWP was transferred to myself and to the CPS, so we now, within our team, prosecute DWP fraud.

Q833 Michael Ellis: So prior to that there was a separate prosecuting entity.
Keir Starmer: Exactly, and one of the areas in which we have all rationalised our business is that we now prosecute for some Departments where we did not before, so we now house and prosecute on behalf of DWP, and that is why it is in our evidence, because it now becomes material for us.

The case here is pretty much the same. There is nothing particularly special about benefit fraud. It is fraud. It happens to be fraud against public funds as opposed to fraud against private funds.

Q834 Michael Ellis: Yes, but we want to stop it though, do we not?
Keir Starmer: We want to stop it and we want to prosecute it; the techniques and the evidence that you use for fraud on public funds is pretty much the same as you use on other funds, and our only concern was that, that being the case and it being the case that DWP currently access the data, again we did not want to lose that capability because it would affect the prosecutions we now bring.

Q835 Michael Ellis: Would it be your submission that the Department for Work and Pensions and thus the Crown Prosecution Service should have access to comms data in order to prosecute benefit fraud?
Keir Starmer: All we are doing is gently pointing out that this needs to be covered in one way or another. I do not think it is really for me to say how that needs to happen; but one way or the other, those charged with this Bill, as it were, should know that the DWP currently has access through statutory provision to this data and uses it; and if, by whatever means, when the Bill is passed, they did not have that capability because it would fundamentally affect the way in which we could prosecute their cases.

Q836 Michael Ellis: So you would not want a limit placed on that body for that purpose.
Keir Starmer: No. The only caveat is that, without studying again the detail of the Bill, I could not say for sure that it could not be achieved by some other means, but by whatever means there needs to be access to that data.

Q837 Michael Ellis: Do you oppose the repeal of Section 109, subsection (2)(a) of the Social Security Administration Act 1992?
Keir Starmer: It rather depends with what it is replaced. If the result is that there would be no provision for gaining access to communications data in fraud on the public purse, then, yes, I would be very concerned. If there is some sensible provision in its place, then no.

The Chairman: I think everyone in this room is happy to see benefit fraudsters prosecuted; it is just a matter of whether we need all the provisions in clause 1 in order to do it.

Q838 Lord Armstrong of Ilminster: The list of authorities that have access to these data under RIPA is very long—10 or 11 or 12 kinds of authorities—and includes not only local
authorities but the Coastguard and other authorities. Do you feel, though, that the use that those authorities make of the powers of access are really much more limited than in the case of the police and the security services? Would you like to see that list reduced? Do you think it is justifiable to use these intrusive powers for these other purposes?

Keir Starmer: I am sorry. I am not sure I am in a position to answer that, because I do not know the use that they put them to or how extensively they use the powers they currently have. I am sorry; there is just a gap there in my own knowledge. I have not had any dealings myself with those bodies in this respect.

Q839 Lord Armstrong of Ilminster: You do not prosecute in all these cases, I take it.

Keir Starmer: No, and, to be honest, I really do not know how often they access it and what use they make of it and, therefore, I am not equipped to answer the question. I do apologise.

The Chairman: Thank you very much, Mr Starmer, for coming along today. I hope we have not detained you too much on your busy schedule. Thank you very much.

Keir Starmer: Thank you. I will follow up on those issues.
WEDNESDAY 24 OCTOBER 2012

Members present:

Lord Blencathra (Chairman)
Lord Armstrong of Ilminster
Lord Faulks
Lord Jones
Lord Strasburger
Nick Brown
Michael Ellis
Dr Julian Huppert
Stephen Mosley
Craig Whittaker
David Wright

Home Office Officials [Richard Alcock, Charles Farr and Peter Hill] (QQ 840-918)

Examination of Witnesses

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, examined.

Q840 The Chairman: Welcome, gentlemen. For the benefit of the public who may be following the events here, to begin with we will be in public session with colleagues from the Home Office. We have a certain number of questions for them. At a later point we will go into private session and ask members of the public to leave as we deal with those issues. We know who you are, but for the record perhaps you would state who you are and what you do.

Charles Farr: I am Charles Farr, director-general, Office of Security and Counter-Terrorism in the Home Office.

Richard Alcock: I am Richard Alcock, director of the CCD programme.

Peter Hill: I am Peter Hill, head of Pursue Policy and Strategy Unit in OSCT in the Home Office.

The Chairman: Colleagues will commence with a number of questions. Do not feel that you all need to answer them if you do not wish to, but also feel free to pile in on any other points if you feel colleagues have not covered them adequately.

Q841 Michael Ellis: Could I start by asking you about consultation with the CSPs, ISPs and social networks in particular? This Committee has heard from witnesses from UK CSPs, who have told us they had had regular high-level contacts with the Home Office in particular but had not been given specific information about precisely what obligations would be imposed on them to enable them to form a view on the extent to which the Bill would affect them. Do you have any comment on that?
Charles Farr: 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. We are also speaking to the various trade industry bodies—ISPA, ITSPA, LINX and so on—where those CSPs are represented. I accept we have more to do on the finer detail of what you might think of as the content of the notices, which, if this legislation is approved, would ultimately be served on the CSPs. From existing conversations with CSPs in the UK, I think they have a pretty clear idea of that, 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.

On ACSPs, particularly overseas third-party providers, with a lot of interest we read several times and closely the two evidence sessions you had with them. I asked Richard to compile a list of all the meetings we had had with those organisations over the past couple of years. There is a total of 30 meetings over a two-year period with overseas providers. It is true that not all of those, because they go back two years, were on the minutiae of the Bill. To be clear, all of them were on communications data.

Q842 Michael Ellis: And on the general principles.
Charles Farr: On the general principles and the relationship we have with them on communications data and in all cases, at some point, on the proposed thrust, direction and content of the legislation.

Q843 Lord Armstrong of Ilminster: You have gone back to the IMP provisions of the previous Government.
Charles Farr: Of course, they would have read all the previous consultation documents issued by the last Government as well, so yes. Our relationship with them goes back to that date, so you are right; these discussions are not new. As to the UK companies, I fully accept that we need another level of detail. It was hard to get to that level of detail before the legislation, frankly. Parliament and others had a right to see the legislation before we discussed it in detail with overseas providers, but I emphasise that there have been 30 meetings over a two-year period.

Q844 Michael Ellis: As far as the UK CSPs are concerned, just to confirm your position, they did accept that they had had regular high-level contacts with the Home Office.
Charles Farr: Yes.

Q845 Michael Ellis: You have confirmed to my colleague, Lord Armstrong, that it goes back quite a way. Clearly, this draft Bill has been in the pipeline, in one form or another, for quite some time.
Charles Farr: Yes.

Q846 Michael Ellis: But you are satisfied that, as far as concerns the information imparted to them and was between the parties in the discussions, they knew about these issues and were working with the Home Office, and they have been.
Charles Farr: Yes, and I think that is reflected in the evidence they gave to you orally. The UK CSPs, as I recall from my reading of it, were fairly clear that the consultation process with the Home Office from their perspective was reasonably good. I repeat that there was always scope for us to get into another level of detail.

Q847 Michael Ellis: As to the non-UK CSPs, if it is suggested that there was no consultation prior to the publication of the draft Bill you are confirming that there have been 30 meetings, so you do not accept there was no consultation.

Charles Farr: There have been 30 meetings with the overseas providers, notably those from whom you heard evidence, over a two-year period on communications data, including some sessions among those on legislation. The degree to which we consulted on the detail of the legislation varies, of course. It is true that with one particular company—perhaps I could name it in the later session, if you are happy—for a variety of reasons we had less consultation than with some of the others. I can explain why that is, if you allow me to do so, after the break.

The Chairman: If we do stray inadvertently into areas which are for the private session, please say so; we will respect that.

Q848 Michael Ellis: We certainly do not want to cause any embarrassment to the companies concerned, but it is helpful that you are confirming the position. This draft Bill would impose some obligations on various companies. We do not need to be specific about company names, but would you accept that potentially it would involve them in some restructuring of their systems?

Charles Farr: Yes.

Q849 Michael Ellis: Therefore, some expenditure will be required.

Charles Farr: Yes.

Q850 Michael Ellis: Where government expect expenditure to be required by third parties it usually makes good those costs, so there will be an allowance for recoupment from the public purse. Is that your understanding of the position?

Charles Farr: Yes. 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.

Q851 Lord Armstrong of Ilminster: 100%?

Charles Farr: We were challenged in an earlier session to ensure we were getting value for money and that the costs were reasonable, but, with that significant proviso, yes.

Q852 Lord Armstrong of Ilminster: But the wording of the Bill does not say 100%; it leaves it entirely to the Home Secretary to decide how much.

Charles Farr: That is true. The CSPs have pointed that out to us and it is a reasonable point. The intention is to cover their costs.
Q853  **Michael Ellis:** Which you say is difficult to quantify precisely.

**Charles Farr:** It can be in some areas, but we want to be open. We have said right the way along that the principle of this Bill is to have co-operation, consultation, and that must include a sensible discussion about costs where they are not immediately apparent.

Q854  **Michael Ellis:** You are satisfied that the consultation and co-operation with the Home Office has gone on for quite some time and to a sufficient extent.

**Charles Farr:** Certainly with the UK CSPs with whom our relationship has inevitably been closer over the years than with their overseas counterparts. We have tried to catch up with the overseas networks, which are very important to us, and I am satisfied that we have a good, co-operative relationship with most of them. I emphasise an additional level of detail is needed in discussions going forward.

Q855  **The Chairman:** If you have had all this dialogue with them, why is it that almost to a man they have said they did not have a clue what the purpose of the Bill was and did not understand what you were seeking to do in Clause 1? The overseas ones have said that they have not had any dialogue with you in any case. If you had all this dialogue, why are they in the dark about what you want to achieve?

**Charles Farr:** I wonder whether in some respects that is a question you may have to ask of them, if I may say so.

Q856  **The Chairman:** We did ask them.

**Charles Farr:** We have had consultation in which we have set out the purpose of the legislation and the main components of it. We got into as much detail as we could at the time the consultations took place. Those discussions were in the context of a wider engagement on communications data. Sometimes the people with whom we have been having consultations were not the people who gave evidence to you, but I cannot speak easily for the CSPs and why they made the comments they did.

Q857  **Michael Ellis:** Do you think it boils down to commercial embarrassment?

**Charles Farr:** It is certainly true—we can discuss it further in the later session, if it is helpful—that companies will understandably be wary, as would we, about disclosing the extent of co-operation they may have with us at the moment and that they foresee in the future.

Q858  **The Chairman:** That is perfectly understandable, and that was why we had a private session with them. In private session they were fairly unanimous that those who had had dialogue with you did not understand what you were seeking to achieve and the nature of the perceived gap. Did you fail to communicate adequately? Did they fail to understand? You can see where we are coming from when some of us would say we are concerned at the level of consultation up until now.

**Charles Farr:** I find myself repeating that we have had 30 meetings with them. All of them have included sessions on the legislation. I have records of those meetings. It seems to me, rereading those records in the light of the evidence, that we gave as good an idea as we could of the thrust of the Bill and its general components. I would accept—you have made this point and others have made it to you—that the language of clause 1 is very general. I think
that is a drafting problem rather than a problem of our intent, and it is one of the things we must take away and look at. We are already looking at it and talking to our Ministers about it. I understand how a reading of clause 1 may not give the precision that the UK, or indeed other CSPs, might want. We are aware of that and need to deal with it.

Q859 Dr Huppert: If I may start by following on the questions about consultation, we have also heard from people like the Information Commissioner—we are still waiting to hear from the Director of Public Prosecutions and the Interception Commissioner—that they did not get much consultation in advance of the Bill. Do you think that is accurate, or are they in some way not giving the Committee the full story either?

Charles Farr: I can explain, if it is helpful to you, the consultation we had with the Information Commissioner. 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. I felt and hoped that the combination of all those steps would have conveyed what we were trying to do. If we failed to do that, as I have to infer we did, we must go back and do it again. It was not for want of trying, and we did have those sessions.

Q860 Dr Huppert: It strikes me how many people there are whose version is so different from yours.

Charles Farr: If I may, we have the records of these meetings.

Q861 Dr Huppert: I am sure we would be delighted to see them, if you want to send them to us. When you came before, you said in answer to Q79, that “major CSPs understand the problem that we are trying to solve, understand the technology and the way in which we are proposing to solve it, agree that that technology is feasible and are looking for legislation to underpin collaboration in the future”. Do you still think that is the case?

Charles Farr: Yes. Rereading the evidence from the UK CSPs, I think that accurately summarises the thrust of what they were saying to you and have been saying to us.

Q862 Dr Huppert: But it is not just the UK CSPs. At Q569 I put that to Yahoo, Microsoft and Google, all of whom explicitly said no; they did not recognise that. They said, “Charles Farr’s characterisation of the conversation is not one that I recognise.”

Charles Farr: But I was referring to CSPs, and I think that in the language we use we tend to refer to over-the-top providers as ACSPs, so certainly my intent in answering that question was to address the UK response.

Q863 Dr Huppert: You mentioned the powers in clause 1. Some time ago we asked to see a draft of the order power in clause 1. You said that the details of the notices were still to be worked up, which presumably means you have looked at the order that would give power to have those notices. Can you share that with the Committee?

Charles Farr: The order.

---

2 Mr Farr subsequently explained that the “meeting” with the Minister was in fact a telephone call.
Q864 Dr Huppert: Yes.  
Charles Farr: That is a matter for Ministers; obviously, they would have to decide on that.

Q865 Dr Huppert: Have you spoken to any of the providers about what the order or notices might look like?  
Charles Farr: Yes. Perhaps I may turn to Richard on that, because he has been having more of those discussions.  
Richard Alcock: We have had discussions about the additional data types that we may wish those service providers to retain, noting that it is going to take a bit of time, should the legislation go forward, for things to be implemented, and technologies and services can change in that time period. Where we are now, there is certain information which is not stored routinely by UK CSPs, in some cases web blogs and in some cases IP data. I discussed earlier the NAT/PAT problem. In the majority of cases, fundamentally it is about those two issues, but there is a broad range of other aspects. It is very much service-dependent in relation to the different service providers in the United Kingdom and overseas in terms of the data we would want them to retain over time as their businesses and services change.

Q866 Dr Huppert: I understand that. Part of my question is about parliamentary scrutiny. Mr Farr said earlier that Parliament should see the information before the providers, and yet you are saying you have a draft order and there are draft notices. You have been talking to people about it, but this Committee, which is supposed to be looking at it, cannot see it.

Charles Farr: I did not say we had the draft order or notices. What Richard was saying is that we are discussing with the providers the data types where we think we might ask them for additional assistance, primarily in the form of retention rather than generation.

Q867 Dr Huppert: If I may move to clause 1 as written, I think you said it was a drafting problem. You have been working on this Bill for four years. It was intended to be part of the Crime and Courts Bill.

Charles Farr: We have been working on it for two years.

Q868 Dr Huppert: I thought you were saying in Q793 that it was related to the consultations under the previous Government.

Charles Farr: Indeed it is, but this Bill is a different Bill, and we were not working on it four years ago.

Q869 Dr Huppert: But something which was ready to be part of the Crime and Courts Bill has a drafting problem in clause 1. You are now saying you might look at that again. Would you look at something specific to fix, for example the NAT/PAT problem Mr Alcock just mentioned? Would that solve part of your problems?

Charles Farr: I have heard that being proposed. 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. The risk in being too specific in the legislation—government may choose to take it—is that you may well have to come back with additional legislation at some point in the near future as data types change and other gaps emerge. Part of our intention with the present drafting was to future-proof legislation to a degree that avoided reverting to Parliament in short order.
On the drafting itself, quite a lot of the questions addressed to the Committee have expressed uncertainty about what types of data we are going to be after. Although we thought the Bill was clear, it could be clearer. We are seeking only those data types which enable us to address the so-called who, when and where of a communication. No other data types are in the scope of this Bill, nor do we want to change the definition of what constitutes who, when and where, although you have raised a question about subscriber information, which is also an important one. We did not quite see that Clause 1 of the Bill was as general and open-ended as others have observed it is, but we want to look at it again, and we must advise Ministers on whether it can be changed, enhanced or improved.

**Q870 The Chairman:** How big a part of your thinking in drafting Clause 1 as wide as it is is the genuine belief that you won’t get a Bill like this every couple of years? It has been 12 years since RIPA. I know from my own experience that the Home Office can get a criminal justice Bill every year but not Bills like this. Hypothetically, if you had a guarantee from the usual channels that every three years you could amend RIPA, would you draft it more narrowly?

**Charles Farr:** I have never known a guarantee of that kind.

**Q871 The Chairman:** I accept that; that is why it is a hypothetical question.

**Charles Farr:** If the Committee can conjure up a guarantee of that kind, we will pocket it and take it away.

**Q872 The Chairman:** I appreciate that you cannot answer; it is a hypothetical question, but it seems to be a large part of your thinking that you have to future-proof this Bill for whatever technology will be invented in five years’ time. Therefore, the Bill is so wide in trying to capture it.

**Charles Farr:** Not five years; that’s the problem.

**Q873 The Chairman:** Two years, three years?

**Charles Farr:** Indeed. You might resolve the IP issue, which I believe has been demonstrated to you, but another issue may well come along very quickly afterwards.

**Q874 Lord Strasburger:** Mr Farr, we have heard a lot from you and others about the 25% data gap. Do you accept that, with the exponential growth in methods and volume of communications data, such data now available to law enforcement agencies is vastly greater than it was in 2000? It is simply not 100% of what might now be available. For example, 12 years ago none of us was carrying around with us what are in effect personal trackers, which other people call smart phones. There has been an exponential growth in the availability of data.

**Charles Farr:** I do not entirely agree with your point. You are absolutely right that 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. That, in a sense, is why we are here.
Q875 Lord Strasburger: We have heard from a lot of witnesses and have been on visits. It has been very clear to us that the vast majority of the data that law enforcement—I have to say we have not been to the agencies—and others want is about the fact of the communication, the who, when and where, and the location which is the bonus that the law enforcement agencies have gained over the last 10 or 12 years.

Charles Farr: That is only what we want.

Q876 Lord Strasburger: Hardly any of the law enforcement agencies we have seen have come to us saying, “We need more.” They have all come to us saying they want to preserve the status quo. They are worried that they will lose what they have got, which is not the intention of this Bill.

Charles Farr: I do not recognise that characterisation of what law enforcement is saying, at least not to us. It does not reflect our own calculations. Perhaps I can talk a bit about the methodology of the 25%, if you are interested. This is not a figure that we have plucked out of thin air. We arrived at this figure by two routes: what I would call loosely a bottom-up route and a top-down route. The bottom-up route, the detail of which we have given to the Intelligence and Security Committee, examines provider by provider working in this country, whether based here or overseas, and the degree to which they are able to retain and provide the categories of data we need to answer those three questions. We have produced that on the basis of input from law the enforcement agencies. That is the first way in which we begin to try to scope the so-called gap and develop the 25%.

We have also approached the problem in a different way by looking at communications trends in general over the next 10 years. What is happening to the communications industry? What type of communications will there be? Which of those types of communications do we know will be relevant to us? What is the current retention for each of them? We have made calculations around that process to check whether the figure we get from the bottom-up process is reflected in the figure we get from the top-down process, for want of a better word. We come up with about 25%, with the direction of travel we have set out in our evidence. The police have had an input in all that work and, as far as I know, are completely content with it. I would be very surprised if, in their evidence to you, they were to say, “We don’t find a gap now and everything currently is all right”.

Q877 Lord Strasburger: The fact is that we have gone in search of the missing 25% of data with every witness we have had before us, both CSPs and public authorities. Almost without exception—there have been one or two—the evidence has been that they could not identify where there is a shortfall.

Charles Farr: My reading of the evidence given to you by the UK CSPs is that to a person they accept that there is a gap. My understanding of your visit to various other authorities was that they had demonstrated that gap. We have given very detailed information to the ISC, company by company and data type by data type, giving percentiles of delivery that we are getting at the moment. We have set out for you in the restricted annex B of our evidence more about the methodology by which we are trying to demonstrate that. We would be the first to admit that these are quite difficult calculations to make, but I believe we have demonstrated the existence of a gap that is currently impeding law enforcement efforts and how that gap will change with or without legislation.
Q878 Lord Strasburger: We have been able to see that there is a gap. We could not identify where the 25% came from, or how it was going to go up to 35% and then down to 15%.

Charles Farr: If there is any further detail we can give to elaborate on annex B and the written evidence, we are very happy to do that. We have given very detailed company-by-company information to the ISC to complement that, and we can follow that up as well. I am concerned that obviously we are not making the case to you with the evidence you are looking at. I can only reiterate that we are happy to provide further material in particular areas, if it would help.

Q879 Lord Strasburger: In the oral evidence the head of EU policy for Microsoft speaking for Hotmail told us that you were unable to articulate what the 25% was because you could not articulate what the 100% would look like. Can you comment on this?

Charles Farr: I was baffled by the comment. I thought our written evidence, which perhaps had not reached Microsoft, was quite clear. The 100% to which we refer is 100% of the data required to tell us the who, when and where of communications of interest to the police or agencies. I said that the 100% is not attainable any longer, and it is not the aspiration of this legislation to get us back to that point because we will not. It was relevant to us only in the era when we all had just BT fixed line telephones. The 25%, therefore, is a reference to the missing data that we would require to identify the who, when and where of communications. I hope that was clear in our written evidence, and I was puzzled by the fact that he did not understand it.

Q880 The Chairman: If you were able to obtain the IP and web log information, how much of the gap would you close?

Charles Farr: Could we do that in the next session?

Q881 The Chairman: By all means; I am happy to do so. On the “who, when and where”, you have said that that is the only thing you are interested in and the only thing that matters. Some of our witnesses are concerned that subscriber data is an old-fashioned definition in the year 2000. Subscriber data can now catch hundreds of things, which allow people to say that this is a wide-ranging snooper’s charter. If the powers under clause 1 of the Bill could be redefined and one was asking only for who, when and where, and you put in tighter definitions of subscriber data, would that give you all or most of what you want, or a lot of what you want?

Charles Farr: We recognise the concern you have identified about the degree to which the term “subscriber data” could expand to suit the data available in a social media provider. Buried in annex F to our evidence, for which I apologise, is an explanation of the data types that we think we mean when we refer to something like subscribers. If I may, I will read it out: “Subscriber data includes name, date of birth, billing address, delivery address, contact information and account reference.” It does not include some of the things that the social media networks might now have as a subscriber. We do not want that material; it would be disproportionate to try to obtain it, and we are happy to go back into the legislation and see if we can circumscribe that. It is certainly not our purpose.

The Chairman: That is very helpful, if I may say so.
**Q882 Stephen Mosley:** Early on in our discussions on the draft Bill we were told that the total cost would be approximately £1.8 billion. Is that the figure you are still working to?

**Charles Farr:** Yes. The business case is being refreshed, and we have mentioned that to you before. I fear that it may be finalised only after the Committee has finished its deliberations, but we do not anticipate it will come up with a figure higher than £1.8 billion. The £1.8 billion builds in quite a lot of optimism bias anyway, which we discussed last time.

**Q883 Stephen Mosley:** I know that when we spoke to the CSPs and other communication service providers we asked whether you had spoken to them about costs, and if they had any estimate of what their costs would be. I am sure you have read the evidence. Pretty much all of them said that there had been either no discussions or very minimal ones on the cost, and they would find it very difficult to estimate what the cost would be. How have you made the estimates of the CSP costs?

**Charles Farr:** As you know, we talk to the CSPs on a very regular basis about their existing data costs; that is, everything that is incurred on our behalf in implementing existing RIPA arrangements. We know in quite a high level of detail what those costs comprise, what the basis for them is and we discuss them regularly. Those discussions and the data we have already have 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 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—we have read the evidence and reconsidered it since then—that these figures accurately represent the likely cost going out to 2020.

One of the reasons CSPs are uncertain about costs is that, at least in their conversations with us, they are very uncertain about any obligation we might place on them in regard to third-party data. I had a meeting last week. I think they were under the misapprehension that we might go to them to collect third-party data, even before asking the third-party to co-operate 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.

**Q884 Stephen Mosley:** One figure that shook us as a Committee was when the guy from Twitter said that it took three years and two months to go from one tweet to a billion tweets, and now they take a billion tweets every two and a half days. What sort of growth in network traffic are you working into your figures?

**Richard Alcock:** We are assuming a growth in network traffic by a factor of 10 over a 10-year period, but I should stress that in the case of certain communication types, for example tweets, within a tweeting session there may be only a need to understand the communications data related to one tweet in a particular session. While the growth might be exponential, that curve may come down quite significantly by virtue of the fact that the value of the who, when and where can be attributed to just one tweet within a tweeting session, if that makes sense.
Q885 Lord Strasburger: Did you say it was a factor of 10 over 10 years?
Richard Alcock: A factor of 10 over 10 years.

Q886 The Chairman: Mr Alcock, do you have anything else to add to that?
Richard Alcock: I must put this in context. This is all about the amount of information that is of value to law enforcement.

Q887 Michael Ellis: It is not all about volume.
Richard Alcock: It is not about net volume over a 10-year period.

Q888 The Chairman: But they have to store the whole volume so that you can find the little bits you want.
Richard Alcock: No; they have to store only the information that we require of them that is of investigative value.

Q889 Dr Huppert: You just said that the costs of the current scheme were based on the idea that most of the problems would be solved essentially by collaboration with overseas providers.
Charles Farr: That is right.

Q890 Dr Huppert: Presumably, that means that if those collaborative discussions—I am still not quite clear how the Bill requires those—are not successful, the cost would necessarily go up quite significantly. Is that what you were just saying?
Charles Farr: That depends on how we responded to the lack of success of the collaborative discussions, doesn’t it? The costs would go up if we had relationships with providers overseas which were not very collaborative, which is not the case, and, having developed such relationships, Ministers decided to revert to a request for a UK CSP to collect third-party data off their network. There are quite a lot of ifs and buts in there, and it is not inevitable that the costs would go up if we did not get all we wanted from an overseas service provider.

Q891 Stephen Mosley: One of the things to which the CSPs referred—you have now concentrated on it—is the cost of storage of the data. They were saying that they had an awful lot of other costs, such as engineering, secure storage and safe destruction, that they could not quantify and they believed you would not be able to quantify. Have you included those costs in your estimates?
Charles Farr: We have—all of those.

Q892 Stephen Mosley: If so, how have you reached those estimates?
Charles Farr: On the basis of the existing financial discussions we have with data providers and on the basis of consultation with other people involved in whichever part of the engineering process we might be discussing.

Q893 Lord Armstrong of Ilminster: One of the people we took evidence from was the Information Commissioner who was very demure, not to say non-committal, about the need for the Bill. He said that was somebody else’s business, not his. I was reminded of the Light
Brigade; his not to reason why but to do or die. But he was much more exercised about the cost of the extra resources he would need to do what the Bill asks him to do in Clause 22(5). Have you consulted with him on what extra resources he might need, and are they factored into your cost estimates?

**Charles Farr:** 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.

**Peter Hill:** That is the sum he estimated.

**Lord Armstrong of Ilminster:** It is in the cost estimates you have given us.

**Q894 Lord Faulks:** On this particular point, the way it is framed in the Bill is to keep it under review. He has to keep quite a lot under review, and that was his concern. He was not quite sure exactly what he had to keep under review at the moment.

**Peter Hill:** The Information Commissioner has responsibilities as set out in the Data Retention Regulations. We do not think that substantively the responsibilities in the Communications Data Bill are very different. There may be more providers or more data, and he may, as is entirely his prerogative, want to perform those responsibilities differently, but, if one looks at the regulations that make him responsible for monitoring the application of the provisions of the regulations, which relate to the security and destruction of data, and you then look at Clause 22(5), which relate to the security, integrity and destruction of data after 12 months, in essence those are the responsibilities that he has under existing legislation, whether it is the Data Protection Act, Data Retention Regulations or PECR. In terms of responsibilities, to us they are substantively similar. If there are more companies retaining data or more data retained, I understand he feels he may need more resource to deal with that, but in terms of how he performs the role, it is a matter for him, but there is no reason to believe that in essence it is a different role from the one he currently has.

**Q895 Lord Strasburger:** Your estimate is that it is £15,000 a year.

**Peter Hill:** No. His estimate is that it would be £150,000 a year, but we have not had the chance to go through the business case for that in detail with him.

**Q896 The Chairman:** You have estimated the cost to be £1.8 billion, but the benefits are estimated to be about £6 billion. It would seem that among those benefits the saving of life can range from £2 billion to £3.3 billion, if we read your figures correctly. This is on the basis that in 25% to 40% of instances where there is a threat-to-life situation when making an application for data a life might be saved. That is between 1,100 and 1,800 people over the next 10 years. Forgive me, but I find all those figures rather fanciful. How do you come to those calculations, and why the wide divergence between £2 billion and £3.5 billion?

**Charles Farr:** We are dependent for these figures on the law enforcement agencies whose job it is to deal with threat-to-life situations. Therefore, these figures draw on their data. We are advised, in consultation with a range of police forces, that in what is described as a threat-to-life situation the number of occasions when a life is actually at risk and is saved varies; it varies from force to force and type of emergency service to type of emergency service. We can get one set of figures from the Met with the resources at their disposal and the geographical area that they command, and we will get a different type of figure from a rural police force dealing with a slightly different type of situation over much different and wider geographical areas.
When I put your question to them, that is their explanation back to me: it depends on the type of force that is engaged in the threat-to-life operation. We are repeating to you the bandwidth of the variation that we have been given, which is 25 to 40.

Q897 The Chairman: That is helpful. We may be able to take it up with the police next week. These are largely police rather than security service figures.

Charles Farr: Absolutely.

Q898 The Chairman: They average about £1.7 million per person. I can accept that for each of us if we lose a loved one £1.7 million is not much; we may value their lives more than that, but it seems to be rather high if the police are saying that if a life is saved in a threat-to-life situation it saves them £1.7 million.

Charles Farr: I do not think we were making that point. If it looks as though we are, we are taking you down the wrong path. I think the answer to is this in the annex to our written evidence under benefits. Colleagues may recollect better than me that the figure we took for the value on a life reflected a Treasury figure used in a number of different scenarios across government. We are given that and we do not really debate it.

Q899 Lord Strasburger: Who would bear the cost if that life is not saved?

Charles Farr: I would have to go away and look at the Treasury methodology. We can come back to you on that. It is a conventional figure.

Q900 The Chairman: Could I press that in another way? It may be something we need to challenge in other areas of government. The cost of £1.8 billion to implement it is paid by the Treasury, or the taxpayer. If there is a saving because people do not die, the Treasury does not get that benefit; that is a saving to my family and other families who have not lost a loved one. How do the Government get the income from someone who is living when they have to bear the cost of £1.8 billion to implement the Bill? Am I making myself clear?

Charles Farr: Yes, but you are going to Lord Strasburger’s question again. Unless colleagues can help, I have to revert to colleagues in government to try to get the answer you want.

Richard Alcock: There is an explanation within the Home Office report dated 2003-04, which I referred to in our last evidence session. That goes through the methodology and what factors are taken into account and where the savings are accrued. We have tried to summarise that on page 77 of our written evidence. The reference to the report is there.

Charles Farr: If it is helpful, we could send you a copy of that Home Office report.

Lord Strasburger: For clarification, can you confirm that these figures relate to the benefit to be derived from increasing the availability of data from your estimate of 75% to 85%, i.e. if this Bill were enacted, or is it a wider figure? Is this the incremental benefit of implementing this Bill, which the £1.8 billion cost is certainly intended to be?

Q901 The Chairman: It is a 10% improvement in closing the gap.

Charles Farr: Again, the answer to this is in an annex to our written evidence.

---

[^1]: [http://webarchive.nationalarchives.gov.uk/20110218135832/rds.homeoffice.gov.uk/rds/pdfs05/rdsolr3005.pdf](http://webarchive.nationalarchives.gov.uk/20110218135832/rds.homeoffice.gov.uk/rds/pdfs05/rdsolr3005.pdf)
Richard Alcock: Fundamentally, the proportion of the benefit in terms of lives saved is accrued by virtue of implementing the Bill and achieving the objectives over a 10-year period, so we can save those lives over that period by virtue of implementing the Bill.

Q902 Lord Strasburger: So there is no inclusion of the benefits derived from RIPA at the moment.
Richard Alcock: It is the net benefit.

Q903 Lord Strasburger: It is the increase.
Richard Alcock: It is the delta by having the Bill.

Q904 Dr Huppert: Following on from that question, the figure in your annex goes up to about 2,000 lives in round figures. If you are saving 2,000 lives over 10 years with a 10% increase, a rough calculation suggests that you are saving 1,500 a year with the 75% data that you currently have. If that is the case, I would hope you would be able to substantiate a saving of something like 1,500 lives a year—it will not be the exact number, of course—using current communications data. Do you have figures to support that?
Richard Alcock: We got this information from law enforcement. They have given to us estimated figures for the number of lives that could be saved by virtue of the Bill over a 10-year period. I do not have the figures to hand showing how many lives are saved right now, but in terms of the proportion in threat-to-life cases where there is that benefit they have given us those estimates and we have had them validated.

Q905 Dr Huppert: Estimating is always tricky. In this case we have the great advantage that we can look backwards on what we have done with communications data. We have heard from everybody how well used communications data currently is. The Met were very keen to defend that rather than push for more. Can you find out figures about the number of lives saved currently using CD, because if your argument is consistent one would expect something like 1,500? I do not expect it to be precise. There should be well over 1,000 lives currently being saved using communications data. If that is not the case, it is hard to believe we will get something more.
Richard Alcock: We have to think of this in terms of a 10-year period. We are talking about 2,000 lives over a 10-year period.

Q906 Dr Huppert: What I am saying is that, if a 10% increase in data availability saves 2,000 lives over a 10-year period, over the last 10-year period there should be something like 15,000 lives saved based on the 75% that there already has been. I do not mind whether we do it annually or over 10 years, but, if you can find the 1,500 a year or 15,000 over 10 years, that would give this Committee much more confidence that you can project to 2,000 over the next 10 years.
Richard Alcock: We are not talking here about 1,500 but a net benefit of 2,000 lives over a 10-year period by virtue of the arrangement put in place. I would say that on average that is 200 a year.
Q907 Dr Huppert: I realise what you are saying, but do you understand what I am trying to say, which is that we have been using communications data? As we sit here communications data is being used presumably in exactly the same way to save lives. If the estimate of 2,000 over 10 years is about right, we should be able to make an estimate backwards.

Charles Farr: I understand the question. One of the issues to come out of your scrutiny and our work for it has been the need for much better information about communications data. I completely accept that. We are talking to the police so that going forward we will be able to address some of the questions you have asked, for example to how many people these communications data requests refer. That is a key question we must be able to answer. The question you are raising now is another one, and I entirely accept that we should be able to answer it if the business case is credible. We have to go away and see what they have, but we must make sure we organise ourselves so we can answer that question routinely in the future.

Peter Hill: Putting those numbers to one side, it is a public figure; it is in the report of the Interception of Communications Commissioner. There are between 30,000 and 35,000 urgent oral requests a year. The vast majority of those are threat-to-life situations, and a significant number of them will result in vulnerable individuals being saved. I do not think the figures here, whatever the underpinning methodology, are inherently implausible when you see just how many authorisations are going on for threat to life on a daily basis.

Q908 The Chairman: All I am challenging is: how do the Government, taxpayer, Treasury and society benefit by £1.7 million if a child is saved? I can understand how the family would benefit; it would be hundreds of millions if a child was saved.

Charles Farr: We deal with a standard Treasury methodology which is set out in a document which we will send to you. I understand the point, and it is important. As part of our work on better collection of data in the future, we will factor that in.

Q909 The Chairman: If we are to question this further, would the figures be trawled from ACPO generally or each police force?

Charles Farr: Not ACPO generally.

The Chairman: So it is from each force.

Q910 Lord Jones: Nobody said Mr Gordon Brown would be to blame for the figures we have just had. I just wish Simon Jenkins, a well-known contrarian, could be a witness here and comment on the evidence I have just heard. However, this is simple. You have said in your written evidence that costs and benefits will be subject to change and are being reviewed as part of the revised business case. Has that review already begun? Are there any indications of what the outcome might be? Will the review take account of the cost to service providers?

Charles Farr: The answer to the three questions is yes. The review has already begun. Richard will have the detail, but the business case, subject to the approvals process, should be with us very early in the new year. Are there indications of what the outcome might be? May I leave that to Richard? Will the review take account of cost to service providers? Yes.

Richard Alcock: In terms of any indication, the review is at an early stage. I think it is very unlikely that the figure will exceed £1.8 billion.

The Chairman: Thank you very much for concise questions and concise answers.
Q911 Dr Huppert: I was going to ask about subscriber data in general, but you have already addressed this. I think there is an understanding that it needs to be a well-defined rather than open definition.

Charles Farr: Yes.

Q912 Dr Huppert: Related to that are the definitions of use and traffic data. I hope you accept that they also need very tight definition on the face of the Bill. There is also an issue about the relationship to content. The definition on page 63 of the Bill is fascinating, in that you state it specifically excludes content but traffic and subscriber data do not explicitly exclude content. Is this just a drafting error, and it should be absolutely clear that anything that is content should be excluded?

Charles Farr: Yes.

Q913 Dr Huppert: How sure are you that there is a crystal-clear definition of what is and is not content?

Charles Farr: The Committee and you are well aware of the debate on this. We continue to believe that there is a sufficiently clear definition of data and content to make this Bill legally viable.

Q914 Dr Huppert: Would you envisage achieving that by having a list of which fields are counted as what, for example? Would that resolve the problem? Otherwise, you will have the same problem of broadness whenever there is a grey area.

Charles Farr: You will have ideas on this, and we would be interested to read them and take them away. I emphasise again that it is not the intention of this Bill to engage in some sort of scope creep. We are simply after those data types which enable us to answer the three key questions: who, when and where. We want to ensure that we do not get into subscriber data of a rather recent kind: social media subscriber data. There will be other areas where we must ring-fence to stop encroachment as well. We would be very interested in any ideas that you have. We are certainly looking at this now.

Q915 The Chairman: You would not be opposed to a revised Bill which said in schedule 1 that subscriber data is XYZ and content is ABC, provided it was reasonably future proof, or gave you what I think you call information of investigative value.

Peter Hill: At the moment, there is a hierarchy that gets you to what you mean by each of these in day-to-day detail. At the top level you have the legislation; at the second level you have the order; at the third level you have the notice; and at the fourth level, which you have probably all read, you have the statutory code of practice, which sets out in rather laborious detail what is meant by subscriber information, traffic information and service use information. It does not set out what content is, because content is everything that is not the categories you have just defined. Whether one can introduce into the primary legislation some of the things that are in other bits of the package is something we will have to look at.

Q916 The Chairman: Do you think it might reassure those who call this Bill a snooper’s charter and say, “Clause 1 is wide open. We know what the Home Office says in private—that it is only after these tiddly bits—but clause 1 allows the whole world to be captured”? Do you
think it might reassure the public if you were able to define the Bill—subscriber, content and so on—more closely?

**Peter Hill:** As I understand the evidence given to the Committee, the primary concern about the scope and the definitions related to the ability, which appears to be in this legislation, for us to require the generation of all forms of subscriber information that a person might normally consider to be content, or things they never envisaged they would be providing to a company in order for them to provide a service to them. It is probably fair that the combination of the generation provisions in clause 1, with the general definition of subscriber data on page 63—in whatever clause it is in—without taking into account the underpinning code of practice and order and notice—

**Q917 The Chairman:** The orders are secret, which also unnerves people.

**Peter Hill:** Notices are secret, not orders. But the code of practice is publicly available and contains a considerable amount of detail about what we mean. I accept that the combination of that generation and definition of subscriber data can lead to the concern that, while the notice may be very specific, as Charles has set out, the possibility nevertheless exists that if a future Government—

**The Chairman:** Even the current Government.

**Peter Hill:**—wanted to require a CSP to generate subscriber data on any number of issues, from colour preference to favourite TV programme, in theory they could, which is absolutely and clearly not the intention of the Bill.

**Q918 The Chairman:** I will not put words into your mouth—we may press this later—but you seem to be indicating that if somebody could come up with better definitions to give you the information of investigative value and cut out the rest, you might be reasonably content.

**Charles Farr:** Yes.

**The Chairman:** Thank you very much.
Evidence heard in Private

**Home Office Officials [Richard Alcock, Charles Farr and Peter Hill] (QQ 919-933)**

**Chair:** We are now in private session. I think it is clear that we will have a transcript for our private use. We will show it to you, and if there are parts of it that are suitable for publication, then we will publish. We would not want to redact all of it if we can possibly avoid it, but clearly, some of it will have to be. We have respected those confidences before, and we shall do so again. Moving on, then, to the first of the private session questions—Lord Armstrong.

**Q919 Lord Armstrong of Ilminster:** I should like to come back to questions which we have been skirting in your public evidence, about the data to be retained. Clause 1 is in very general terms, and this is sounding alarm bells, particularly among people concerned with the retention of the maximum amount of privacy, and the human rights aspects of that. It is clear from what has been said today, and previously, that you are not really interested in anything as general as Clause 1 now seems to say.

As you said this afternoon, and in restricted evidence elsewhere, the two specific types of information you want to get hold of, if they are not where they are now retained, are subscriber data relating to IP addresses—that is who is using an IP address at any given time—and, secondly, data identifying which services or websites are used on the internet. That is briefly, succinctly, defined as the weblog up to the first forward slash.

We are beginning to understand that the reasons why you do not want to be specific about that are that you would be sending a signal to criminals and others that those were the data you would be particularly concerned with, and would therefore provide them with a reason to try to avoid them. You have gone a very long way in the Home Office to say that these are the two categories of data which you want to be sure of getting. I do not know whether you can tell us if it is 90% of the general, 80%, or another percentage, but they are the main things. There may be problems of definition, but such problems can usually be overcome by drafting. If there is a problem with the security, is it not really sufficiently breached to make that of concern? Even so, could those you might call the ungodly not work out pretty easily for themselves that that is what you would be interested in? So I think that we would like to press you to say why we should not amend Clause 1 to say that the data you want to be retained and collected are the subscriber data relating to IP addresses, and weblogs up to the first forward slash. There may be problems of definition about that, but such problems can usually be dealt with.

I think we all think that if you could restrict Clause 1 in such a way, it would make it very clear that what you required was for genuine purposes of law enforcement and public protection, and that there would not be a fishing expedition for all the data. That would be considerable reassurance to those who are concerned about the privacy aspects that the data you were acquiring were for genuine law enforcement and protection purposes.

**Charles Farr:** I will cover two or three points. First, I just want to reiterate in closed session what I said in open session, because it remains entirely true, that the only data types we are interested in having retained are those which enable us to answer the three core questions: who is communicating, when are they communicating and where? It is also true that two of the key areas which inhibit us are IP resolution and weblogs, but in the annex to our written
evidence to you, we do of course mention the third area, which is third-party data. I
appreciate that that is the subject of a slightly separate conversation, because it bears on the
whole issue of this legislation interacting with overseas providers. But there are three areas,
and three key gaps rather than just two: IP resolution, weblogs and third party data.
There are some other areas which Richard or Peter can talk about in addition to those three,
which are also important to us, but perhaps less important than the three core gap areas. The
fundamental reason why we are nervous about limiting Clause 1 is future-proofing.

Lord Armstrong of Ilminster: What?

Charles Farr: 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. 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. It does not say that perhaps as specifically as it could. But I still worry—the
others can comment—about something that is quite as specific as what you have in mind.

Peter Hill: You tell a draftsman what the problems are that you want to fix, and they give you
a draft back. It is not clear to me what element of Clause 1 is considered to be too broad. I
understand that generating subscriber data is one issue that bothers people. But if you want to
resolve IP addresses, you need to be able to do a number of things. If you want to get weblogs,
and to get third-party details, you need to be able to do a number of things. Those are caught
by the Clause 1 provisions, which are about the collection, retention, processing and
generation of communications data, in order to give you as Charles says, those three types of
communications data. So you are only requiring companies to do it in order to produce one of
those categories of data. That is the, “Who, where, when, how?” constraint. As Charles says,
those are the three core issues. There will be others, that we have not spotted now, that in two
or three years will be the next IP resolution.

Q920 Lord Armstrong of Ilminster I take the point about future-proofing, but as you just
said, it is very difficult to future-proof in this area, where the future comes upon us very fast,
and very often in unforeseen or unforeseeable forms. Is there any future in provision which
said, in whatever the right language is, “These are the forms we want: the subscriber data, the
IP addresses, the weblogs and the third-party data. If, in the next X years, something else
comes up, the Secretary of State has power to introduce an affirmative order to add to the
list”?

Charles Farr: Well, it is obviously for consideration. I think there would be a risk that we
would advertise to people to whom we would rather not be advertising, the existence of a gap,
which would then prove very popular.

Lord Armstrong of Ilminster I understand that, but when we went to see the Metropolitan
Police I was impressed by one senior officer, who said that we should be surprised at the
number of people who do not really fuss about it, but use communications without encrypting
or taking the kind of precautions you would take to avoid detection. That officer was, I think,
of the opinion that that was a problem that could be set to one side.
**Charles Farr:** We have indeed always said that to you in this Committee. When you have presented clever technical reasons to us we have replied that they are clever technical reasons but not everyone is aware of them. It is true that many criminals, including terrorists, use communications tools in a very simple way and may not be aware of some of the gaps that we are talking about. But that is not universally true. If you took evidence from the Child Exploitation and Online Protection Unit it would not be saying that. It would be saying that that type of criminal is completely aware of where we are vulnerable, will read the contents of this Bill with great interest, read the deliberations of your Committee and behave accordingly. So it is not universally true that criminals are, in communications terms, unsophisticated and that we can do things in front of them without their noticing it.

**Lord Armstrong of Ilminster:** We are already in that state. You have already said so this afternoon, you said it in your written evidence and there is a UN report that quite recently came out which itself refers to these forms of data. Reference to it in a clause in legislation would hardly be adding very much to our knowledge or understanding.

**Chair:** It would seem from many people who have given evidence—and the Home Office has been very secretive on this as it does not want to tell the bad guys what we are up to—that we know exactly what it is. It is IP addresses that it needs; it is weblogs. We know the companies who will have orders served on them. They will be the big six; there will be BT and Vodafone. They say there is no point having such paranoia to keep some things secret when we know who they are getting at. I am merely adding to Lord Armstrong’s point that, if we were to use an order-making power, there is a danger that if the Bill says we are after XYZ and then in two years’ time the Home Secretary adds AB to it, you identify what you are after but many out there already know.

**Charles Farr:** I have read the evidence presented to the Committee. I often ask myself: how many times have these people giving evidence to you investigated a terrorist attack? How many times have they conducted an operation against terrorists? With respect, they seem to know almost nothing about how we have to proceed. I do listen to what they say with great respect on technology and the commercial aspects of this, but I am really not sure that they should presume to give us advice on the investigation of terrorism in this country, or indeed on child exploitation. The police officers who are responsible for that have made their views very clear. I absolutely accept that there is a group of criminals, including some terrorists, on whom this debate will make no impact and who will carry on using simple tools—probably just a mobile phone—and long may that continue. I emphasise that they are not the totality of our target.

**Q921 Lord Strasburger:** Is it not the case that the sophisticated ones that you are referring to will use some of the avoidance techniques—encryption, VPNs and so on—in any case, so they will get around whatever provisions you put in place?

**Charles Farr:** They will try to do that but, as some of your witnesses have implied, we can deal with some of it and much more than they think.

**Lord Armstrong of Ilminster:** You have to balance the risk that some people will, as it were, see what you are up to and take evasive action against the other risk from the current Clause 1 of people who think that this is massive assault on privacy with no sufficient justification in terms of law enforcement. So there is a balance to be struck.

**Charles Farr:** Of course.
Lord Armstrong of Ilminster: We are obviously looking at where that balance should be struck.

Charles Farr: I entirely agree. We are, after all, dealing with some other aspects of counterterrorist legislation—TPIMs versus ETPIMs, 14 days versus 28 days. It is not a completely dissimilar debate.

Lord Armstrong of Ilminster: Some of us know about that.

Charles Farr: I try to put ourselves in the position of our successors—or of us—in two years’ time when this legislation may be through but a gap is opening up and we do not know how quickly we can fill it. That is a really hard position for the agencies, police and Ministers to find themselves in.

Peter Hill: In terms of the timing that we work on and the timing that technology works on, our best guess is that Royal Assent for this Bill, were it to be approved and agreed, would be some time in early 2014. An order might be approved some time in the summer or autumn of 2014. We would then be rolling out notices in early 2015 and we would start having the capability to deliver from 2016 onwards. On the basis of this Bill, the situation in four years’ time will already look quite different from the situation we are facing today.

Q922 Michael Ellis: Even with this Bill, you are talking about a four year delay before things can really apply and technology—based on the past four years—is likely to have taken us on further from that. Is not the nub of this that we are not dealing with minor mischief here? We are dealing with attempts to defeat serious criminal activity: terrorist activity, child exploitation and paedophile activity. I think you have accepted that not everyone is going to be using the sort of technology which will be met by this Bill or similar legislation. But it will defeat many of those individuals and these are not individuals to be sneezed at. We are dealing with very serious offences and if we can defeat one of them it is a very significant achievement. There seem to be questions predicated on issues of achieving 100% success. Very few things done by government or anybody else achieve 100% success. But are you satisfied that a lot of the mischief that we are seeking to address in law enforcement would be met by these measures?

Charles Farr: Yes. We are debating two or three things here. We certainly believe that legislation of this kind, if passed, would address a significant chunk of the problem. Secondly, we would rather not get into a position where we have to come back in fairly short order—particularly because the Bill will take time anyway—and seek a further measure if they were to be specified on the face of the Bill. Thirdly, it is also true that some people follow these debates in great detail and would benefit from seeing us doing it.

Q923 Chair: As Mr Ellis has said, you are dealing with serious issues here: counterterrorism, paedophiles, serious crime. Would you, therefore, be happy to dump the 600 other public authorities that have climbed on back of this Bill over the past 12 years and can, theoretically, access the data? There are some important ones: UKBA with 10,000 applications, the FSA, HMRC and all the rest, my favourite being the Defra egg inspectorate, which has the right to check whether the little lion is right. Would you dump those, Mr Farr?

Charles Farr: As you know, the Government have taken a very clear view on this.

Michael Ellis: We should ask Edwina Currie.
Charles Farr: The Government have put four organisations on the face of the Bill and have asked the rest to make their case. That is a pretty good way to proceed. They are making their case as we speak.

Chair: Slowly.

Charles Farr: Yes, and some of them are making it better than others.

Lord Armstrong of Ilminster: You can say that again.

Charles Farr: It is very likely that numbers should drop, is it not? It is ultimately a matter for Ministers, and you will have your view.

Chair: Or possibly build in additional hurdles for those others.

Charles Farr: In fairness to them, to the number of times that they have actually used it is of course very small.

Chair: That is true. Some have never used it.

Lord Armstrong of Ilminster: That argues both ways really, does it not?

Peter Hill: If they used it very little, should they have the power removed because they use it responsibly?

Chair: Critics have looked at Clause 1 and said, “My God, the Government can catch everything”. Then who is allowed to do it? Well, MI5, MI6; we can accept that. Then they find 600 other miscellaneous organisations. Cutting off the local authorities, who of course should be cut off, does not answer that question: the Government are going to capture everything, theoretically, and everyone is going to get access to it.

Charles Farr: You can see the Government’s drift from the fact that four organisations have been put on the face of the Bill, and the rest have been asked to make their case.

Michael Ellis: That’s a different view from if people were getting salmonella from egg poisoning.

Charles Farr: There are some among the minor users who have a good case, actually, but not all of them.

Q924 Michael Ellis: Do any UK CSPs currently keep the data needed by the law enforcement agencies on IP addresses and web logs? If so, why do some and not others?

Charles Farr: Yes. Why do they vary? Because business practices vary and sometimes their idea of what might be required in future varies, and they may decide to build in that case.

Michael Ellis: Have we asked those that do not to start doing so voluntarily?

Charles Farr: In some areas yes, on IP resolution and on web logs, but this comes back to the point I have made to the committee before: that many will turn round and say that the legislation does not require it, so what exactly is the basis for your request?

Michael Ellis: So it has been your assessment that because they would incur expense or inconvenience, it needed legislation. They are saying effectively that they are not happy to do it voluntarily.

Charles Farr: They do not always need to do it for business reasons; that is the core point. As you know, the key issue in the legalisation is to extend the basis on which we can ask for data that is not required strictly for—

Michael Ellis: And if we relied on them voluntary, I presume you would argue that they could stop voluntarily at any point in the future as well, or fail to co-operate.
Charles Farr: Yes. Also, the legislation provides a basis for payment. Absent the legislation, that is much harder.

Chair: Could you persuade the Treasury to put the words, “There will be full cost recovery” into the legislation?

Peter Hill: In a sense, you can come up with whatever form of words you want. You have still got to negotiate with the company concerned what the marginal cost of the service that they are providing is. The discussions with the company always come down to what the margin is and what might be the margin plus a little bit. That is where the discussion is, whatever the words in the legislation might say.

Lord Armstrong of Ilminster: What you say in the legislation could be different, and could be more or less reassuring.

Peter Hill: It is a starting point, yes.

Lord Armstrong of Ilminster: On the future-proofing, I absolutely understand the point. Since my days in the Home Office, we have got used to having a criminal justice Bill every year. Can you not tag any necessary changes in this legislation on to that?

Charles Farr: Recent experience has been that that’s a fairly long bit of legislation anyway. It is a reasonable point. Whether there would be any coherence is another matter.

Chair: We used to know them as Christmas tree Bills; everyone would hang a bauble on it. As an aside—and this will need to be redacted—Lord Armstrong just lost a bet with me. He asked me why the clause was so wide, and I said, “The Home Office are afraid of future-proofing; they will never get another Bill for 10 years”. We will not want that in any evidence session but you lost your bet. Who else will come in on this point before we move on?

Q925 Dr Huppert: I can understand your concern about future proofing. It is unrealistic to expect Parliament to give a blank cheque. You may want to look ways of future proofing with a serious level of scrutiny. I am sure that you would accept that the level of scrutiny that this Committee is providing is significantly higher than would have happened, as was the original plan, had this gone through as part of the Crime and Courts Bill. How would you have coped if this had just been part of the crime and courts Bill? Would you have had the opportunity to do the reflection that you are currently doing?

Charles Farr: To be honest, I have not speculated on that. I have got my hands full working out what should be doing now.

Q926 Dr Huppert: With these three areas that you have identified now, can make sure that I understand quite clearly, for each of them, you are going to let us know later exactly how much of the gap they would fill. But there is also this issue about how much legislation is required. You say that quite a lot of the companies already keep some elements of it, so they are clearly allowed to do it. There could presumably be a financial structure set up. You are presumably allowed to pay them for services without this piece of legislation, or am I wrong in that?

Charles Farr: To be absolutely clear, the legislation at present requires companies to retain only such data as they require for their own business. They do not require this for their business, therefore we have no mandate with which to go and obtain it, or pay them for it formally. So that is what we need.
**Dr Huppert:** The same would apply for overseas providers, who do provide you with data and who you pay money to at moment. Or do you not?

**Charles Farr:** Overseas providers do provide us with data at the moment, and if I may say, one of the impressions generated by some of the evidence is that they do not provide us with very much at all. Of course, some of them do. I can understand why some of the people giving evidence to you were a bit puzzled at the suggestion that they do not provide all we want.

**Dr Huppert:** Who does not?

**Charles Farr:** I do not really want to get into the names and details. We have provided it all to the ISC. To go back to the UK point, which I have drifted off, I really genuinely believe we need this legislation, because we need to extend the parameters beyond what CSPs collect for their own business purposes.

**Chair:** We are a bit bogged down here, gentlemen. I will move on to Lord Faulks, but Lord Jones had a point on this.

**Q927 Lord Jones:** Lord Armstrong really triggered off this encounter when he used the word “balance”—you know, state security and the rights of the citizen. The promulgation of your Bill is a really big step in terms of our nation. Are we sure your team and Ministers have debated at length this need for balance?

Secondly, you initially used word “terrorism”. That is not a criticism, but shall we presume that the security services have made a big input to you as the Home Office as to what they require? In their needs, shall we presume also that they need, as security services, in terms of the Bill and what is in it, to reassure their helpful counterparts in, say, Washington, that they and the Home Office mean business where terrorism is concerned?

**Charles Farr:** On your first point, in my experience, Ministers in the Home Office are always very alive to the need for balance, in this case between issues of privacy and issues of public safety. That is a very easy thing to say and a very hard thing to achieve.

**Lord Jones:** It seems always to be said by people like you.

**Charles Farr:** Yes, and I absolutely confirm that those issues are constantly in our mind. We went through an entire review of our counterterrorist legislation, fundamentally, with that balance in our mind. That led, as you know, to the repeal of Section 44; the withdrawal of stop and search without suspicion; the change in pre-charge detention periods; the abolition of control orders and the move to TPIMs; and the attempt to strike that balance rather better than we had. We are still working on other aspects of our counter-terrorist legislation; for example, is Schedule 7, which stops people at borders, too indiscriminate? This principle, a balance between public safety and privacy, is constantly with us and is reflected in the work that we have done. On your second point, the Security Service has given evidence, of course, to the other committee. I know that you wanted to talk to them. They strongly support this Bill. Not just in their own right because they need it, but remember—if I may emphasise this—they depend on an effective police force. The Security Service has no power of arrest. It is the police who have to make the arrest and prepare a case against a terrorist operation and, indeed, for serious crime as well. The police need this even more, therefore, than the security service does.

**Q928 Lord Faulks:** On that point, you’re striking a balance, are you, in human rights terms, between the obligation under Article 2 and the obligations under Article 8? There is quite a
detailed memorandum by the Home Office attached to the Bill in that respect. What I wanted
to ask you was this. I think that it is fair to say that it was a constant theme of your evidence to
us on the last occasion and now and, indeed, of your helpful written evidence, that the
purpose of the legislation—I am quoting a particular passage, I do not think out of context—is
to facilitate closer co-operation and collaboration with CSPs in the UK and overseas, to enable
the police and others to access the data they require. Just supposing you do not get this Bill,
you are still going to be committed to try and promote the collaboration and co-operation.
Part of your cost estimation actually embraces operational enhancements within the limits of
the current legislation. What I want to know is, how much of what you want can you get
without legislation?

Charles Farr: Richard, do you want to have a go at that?
Richard Alcock: Sure. Effectively, the legislation is needed to fill the gap. We are doing
everything we can do now, which has been articulated, hopefully, in the written evidence
provided, to try and stem the flow, which is growing and which law enforcement, as well as
we, are seeing. We have been training law enforcement nationally for this—something like
5,000 officers. We are working with communication service providers now in the United
Kingdom, upgrading data retention systems when there is a business need to have those data
retention systems. We are putting measures in place for specialist disclosure interfaces to
increase the speed, as appropriate. I assure you that everything we can do, we are doing,
within the legislative bounds. We are trying to be as persuasive as we can be on the business
purposes front. The reality is that there are hard stops and those hard stops can be countered
only by legislation, which enables us to put obligations on.

Peter Hill: I do not know whether it is worth saying that the 25% is a retention calculation. It
does not take into account the fact that particularly, but not only, for some overseas providers,
even if they retain the data, you may not get it in a timely fashion, or a fashion that you can
use. So there is more that we can do with some providers in order to improve the provision of
their data. But the analysis of the gap does not take account of that. So the 25% is just a
retention gap. So whatever else you might do in helpful dialogue with the companies does not
address that 25%.

Q929 Lord Armstrong of Ilminster: To what extent is the need for legislation in order to give
the CSPs the reassurance, or the cover, for voluntary co-operation with their shareholders?
Charles Farr: I think that it is a very important part of it. I refer back to the earlier evidence
that I gave about the attitude of CSPs to this legislation which Mr Huppert quoted earlier on. I
think that they do understand that there is a gap; they do understand why we need to cover
that gap; they believe that the technology is there that would enable us to do so; but they are
not going to do it unless we legislate. They have shareholders and their own board to think of.
Chair: I would like to come back to that.

Q930 Lord Faulks: May I come on to the overseas data gap and the third party data, which I
know is a matter of considerable concern to the Home Office? We’ve had some evidence from
some of the overseas CSPs that they would effectively not co-operate. What evidence do you
have that a notice on an overseas CSP would be effective, and would not in fact actually
damage co-operation—the co-operation we are so keen to encourage? Was there an element of bluff about this?

Charles Farr: No.

Peter Hill: By us or by them?

Charles Farr: Not by us.

Lord Faulks: Do you envisage actually using powers to capture the data from the major overseas company, or is it envisaged that it is going to be restricted to the smaller fry?

Charles Farr: I personally would not want to go down the route of collecting third-party data from a network here without the collaboration of the service provider. It is not in keeping with the relationship we have with the major service providers now and I really do not think it should come to that pass. I can understand, as the UK CSPs have said to us and said to you, that that would put them in a difficult position; and we want to avoid it.

Lord Faulks: We need to see some informal reassurance from you. Can it be built into Bill in some way?

Charles Farr: I said to them that it is an in extremis power. I would draw a distinction between our dealings with major US ACSPs 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 co-operative relationship. I think that it is in that sort of context that we envisage probes (DPI), and certainly not, if we can possibly avoid it, in the context of the major ACSPs.

Q931 Chair: I got the impression from the American CSPs we talked to that, yes, they did want some cover before doing this, but the cover wasn’t so much a cosy understanding with the Home Office; the cover was some legal thing like MLAT, or something else. I think that when they get a notice served by the FBI, there is some legal backer behind it. An American company is conscious of the law and how its shareholders react. I got the impression—I hope I am not wrong but I am not the only one—that they really would have liked some legal cover behind this in the States. So, can you comment on that? Secondly, if it will take until 2014, why do you not energise your colleagues in the Foreign Office—and Simon Sheriff, head of counterterrorism, and Sue Hemming, Head of CPS Special Crime and Counter-Terrorism Division, who have signed this UN thing yesterday—to get them to speed up MLAT?

Charles Farr: We have read the evidence. Some of the ACSPs, but not all of them, of course, looked at MLATs as a possible solution. There are two problems with that. MLATs are only useful if the data is there to be obtained. If the data has not been retained in the first place, it does not matter how quickly you speed up your MLATs—you will not find anything at the end of the pipe when you get there. That is part of the issue that we are addressing with the ACSPs. Secondly, on MLATs; the person from Microsoft got this absolutely. 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. Peter can talk you through an MLAT process, if it is helpful, to demonstrate just how many stages you have to go through. 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. Microsoft, in their evidence to you, had this absolutely right.
Chair: Thank you very much. Do you think that there is scope for an international agreement—or perhaps not international, as that is far too long—a special bilateral agreement between ourselves and the United States, where most of these guys seem to be based, which would give you a revised MLAT or a means of doing day to day investigations?

Charles Farr: I am really hesitant about going in that direction. In all the informal dialogues we have with ACSPs they do not mention this. I recognise that it was mentioned in the evidence session. My instinct is to try to continue with the productive collaborative relationships that we have at present, using this, if the legislation is passed, as a framework and a benchmark that we can use to say to them, “Here’s what we’re getting from UK CSPs. We want to get as close to this with you as we can; can we please discuss it?” That is the dialogue that we want, and I think that MLATs would really complicate rather than facilitate it.

Peter Hill: Whatever the process with the Americans might be, it is about access. It is about accessing data. The issue we have is about the retention of data. Many US companies hold the data we want, but they hold it for a month, so by the time an investigator goes to get it, it is gone. We would like them to hold it for longer. That is not a process that an MLAT can help us with. In fact, by the time the MLAT request goes in, the data has been deleted. Usually what will happen is that the investigator will get it quickly, and then some time down the road, when a prosecution is pending, they will put in an MLAT request in order to get it as adducible evidence. Whatever construct you had does not address the basic problem we are facing, which is that the retention periods of UK data for the major US CSPs, in some areas, are too short.

Chair: That is fairly concise, thank you.

Q932 Dr Huppert: This issue about collecting third party transient data is a very sensitive one. You raised the cases for educators, where you might have a very unfriendly Government, and so forth. Section 94 of the Telecommunications Act 1984 gives the power for extremely broad directions in the interests of national security to be placed on Ofcom and any provider of public electronic communications networks. Would that give you the cover that you need for national security cases?

Charles Farr: Well, possibly, but it is not a particularly transparent bit of legislation.

Dr Huppert: You think that we should repeal it as well?

Charles Farr: I did not say that. Of course, you come onto the critical point of whether the information that you are looking for constitutes a threat to national security, or whether it is organised crime, which is not always a threat to national security. So, possibly—but I do not think it is a very appropriate vehicle, and it suffers from the threshold problem.

Chair: Thank you very much. We are almost there. Lord Strasburger.

Q933 Lord Strasburger: On encrypted data, CSPs came out of the separate consultations with you, with conflicting impressions of what you would require from me in terms of retaining encrypted data. Mr Hughes from BT came out with the impression that he would be required to retain it, while the gentleman from Everything Everywhere was very specific that it would be excluded. Which is it?

Charles Farr: We have been clear with the providers—we had them in last week and discussed this specifically—that we will only be asking them to collect unencrypted data. If they cannot
distinguish CD from content they will not be required to retain it. We are not asking for the storage of masses of encrypted data.

Lord Strasburger: Or any encrypted data? Would it not be preferable for such assurances to be written into the legislation?

Charles Farr: We can certainly look at it.

Lord Strasburger: This might be a little irrelevant in view of that answer, but we are told that where data is encrypted—no it is irrelevant so I will not ask it.

Peter Hill: Do you want to ask the question?

Lord Strasburger: So have you got a pre-prepared answer you want to give us?

Charles Farr: No, but there is an important point about encrypted data.

Lord Strasburger: Go on then.

Charles Farr: Once again, we are right at the edge of the sensitive aspects of this. We have discussed what use encrypted data is to us with the ISC and I am sure you are hooked up with them. You took evidence from Malcolm Hutty from LINX—not our greatest fan of course—and what he said about this was exactly as we see it. In other words, 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.

Lord Strasburger: Our understanding from evidence earlier today is that there are two types of encrypted data: the type that has communications data in the clear, and the type that is entirely encrypted. Presumably you are referring to the first category.

Charles Farr: The first, certainly.

Chair: We all take the point. Even if one cannot read a single bit of the message, if you discovered who spoke to whom and when then that, added with other evidence, can give you a picture and possibly something more.

Charles Farr: Or even, by the way, where.

Chair: That is fair enough. Are there any other questions? Thank you very much. The session has gone on a lot longer but it has been most enlightening. From what you are saying, I detect some movement from the Home Office in looking at the terms of the Bill and its drafting. From what you have said today, Mr Farr, it is possible that we may be slightly less critical than we were going to be before we heard your evidence. It has been very helpful and enlightening. Thank you very much and thank you to your staff. I am sorry it has been such a long session but it has been very helpful: more so than you may realise.
Examination of Witnesses

Witnesses: 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

Members present:

Lord Blencathra (Chair)
Lord Armstrong of Ilminster
Baroness Cohen of Pimlico
Lord Faulks
Lord Jones
Lord Strasburger
Nick Brown
Michael Ellis
Dr Julian Huppert
Stephen Mosley
Craig Whittaker

Trefor Davies, David Walker, Caspar Bowden and Privacy International [Dr Gus Hosein] (QQ 1013-1067)

Examination of Witnesses

Witnesses: 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, examined.

Q1013 The Chairman: A very warm welcome to you, gentlemen. Dr Hosein, welcome back for the second time. For the benefit of the public record, we were trying to question Dr Hosein a few weeks ago and we were interrupted by so many votes he did not get much of a chance to give evidence. Just for the record as well, perhaps if you would all state who you are.

Trefor Davies: My name is Trefor Davies. I am the CTO of an ISP called Timico.
Dr Hosein: My name is Gus Hosein and I am the Executive Director of Privacy International.
David Walker: Dave Walker, Managing Director, Labelled Security Limited, but just here representing myself.
Caspar Bowden: Caspar Bowden. I am an independent privacy advocate. Formerly, I was Director of FIPR and, more recently, Chief Privacy Adviser to Microsoft, but I represent nobody other than myself at this meeting.
The Chairman: Thank you very much. We are very grateful to you for coming and we are looking forward to the evidence you have to give us.

Q1014 Dr Huppert: It is very good to see the four of you here. One of the issues that I think a number of you have raised concerns about is how broad Clause 1 of the draft Bill is. It captures a huge range of information. This is related to the Home Office’s claimed data gap.
Last week, we were told in public session by the Home Office that their intention was to use the Bill to plug two specific areas of the data gap: information relating to IP addresses, and information relating to weblogs. If the legislation could be drafted narrowly to only allow notices to capture those areas from CSPs domestically, would that significantly allay your fears about the scope of the draft Bill?

*Trefor Davies*: I take it from when you say “weblogs”, you mean details of websites visited.

**Q1015 Dr Huppert:** Only up to the first slash, as is currently allowed under RIPA, without the identifying features later, but which is not kept currently if it is not for business purposes.

*Trefor Davies*: There are two sides to this discussion. One is the straight technical side from an ISP’s perspective. Many ISPs will already store information of the IP addresses. As a business ISP, we only provide people with fixed IP addresses, and these will not change from one year to the next, to be honest. The bigger consumer guys and the mobile ones may well change them quite often and so, physically, it is probably not too difficult a thing to do. From the weblog information, most small ISPs would probably have to put some investment in technology in order to be able to support it, but again it is not too difficult a thing to get your brain around.

I guess from the point of view of the other side, which is the privacy side, it is whether narrowing down the information to just those two areas significantly reduces the amount of information that you can drill into about a person. We saw some responses in the written responses; one was from the Tor Project, who said that, “23.3% of Wikipedia users could be uniquely identified from the ‘use data’”. You only have to look at the recent news that came out about the Houses of Parliament, that there are only two IP addresses that are used to access the internet from here and that it was possible to see that a number of the Members’ Wikipedia profiles had been modified from within the Houses of Parliament. Therefore, you could say that a lot of information could be gleaned about somebody still if you were drilling into or fishing IP address information.

**Q1016 The Chairman:** Members of the panel, if you have something to say, say it. It is not just one each, but if you have nothing else to add then we will move on.

*Dr Hosein:* Following this revelation last week, we did a consultation with our friends and colleagues in industry, both domestic and abroad. When we spoke with the telecommunications companies domestically, they informed us that already do record the information the Home Office is seeking under the Digital Economy Act, so would not require any of this discussion. This Bill is not necessary for achieving that objective. Talking about weblogs of, say, the providers, the foreign service providers, for instance, when we spoke with some of the major players, whose names I cannot mention, they expressed their concern about the idea of being compelled to collect this information. Although they process it, they do not collect it and they do not store it, and this entire scenario seems to be generated because we are still using IP version 4 and they believe this will all be solved within a couple of years when everybody moves to IP version 6. So it does seem odd that we have this massive piece of legislation with a vague objective to solve such a small problem that, in a sense, is solvable already domestically.
Q1017 Dr Huppert: Can I just bring you back to the Digital Economy Act issue, a controversial piece of legislation, as you know? Are you saying that all of the domestic providers specifically have everything that the Home Office said last week, and would any of these providers, even anonymously, be able to write to this Committee to confirm that? Because I think it would be very helpful if, in fact, they already have it all.

Dr Hosein: Yes. I asked one of the providers for them to say so publicly and they responded saying they already have, in a submission to Ofcom, so in our written evidence the first footnote refers to exactly that public source where they state as much.

Caspar Bowden: I do not know what was said to the Committee in secret session by the Home Office, so I am trying to read between the lines about what information you have received about weblogs and IP addresses. Certainly one aspect of this that I have been concerned with at European level is I have been sitting as an independent expert on the EU committee to implement the Data Retention Directive for the past three years, and this subject has cropped up, as you might expect, in that committee. I will just rehearse and clarify what the issue is here. We are talking, by weblogs, about logs of websites visited retained by the internet service provider and the internet service provider would only be able to do this by, essentially, intercepting the stream of packets en route to that third party website, because, as it were, that traffic between the user’s computer and some other website is, in a sense, nothing to do with the internet provider. The internet provider’s function is merely to convey packets from A to B.

Q1018 Dr Huppert: But it knows, presumably, where B is in order to convey the packet to B.

Caspar Bowden: Not really, because at that level the packets are just datagrams, which are just passing through the internet service provider’s pipes. Sometimes internet providers used to operate something called a “transparent cache” or “transparent proxy” where they would keep copies of frequently requested webpages from all over the internet to save bandwidth, but that is really not done very much now at all. I think the Committee should be clear that this proposal for ISPs to log websites visited is intrusive and, frankly, it lacks a legal basis. There is no basis for requiring this currently, as I understand it, under UK laws or secondary legislation that is currently in force, nor is there any legal basis for doing this under the European Data Retention Directive. Now, there are technicalities in European data retention and the intersection between European and domestic law which might permit this, but it is, I would say, dubious. Indeed, if this is going on today—if internet service providers are retaining information about websites visited—this is something that was discussed by the EU Committee, and European data protection authorities took the view that this was illegal.

Q1019 Dr Huppert: I must say we are getting different messages. Mr Davies says that this is easy to do, Dr Hosein says that it is already legally required, and Mr Bowden says that it cannot be done.

Dr Hosein: I think we are talking about different aspects of it. What I was speaking about was whether or not a domestic mobile phone provider would record the IP address given to a user and the source port that was granted to that user for that moment in time, so that may be recorded by the domestic mobile phone company.

Q1020 Dr Huppert: So not the URLs that they go to up to the first slash.
**Dr Hosein:** Caspar is addressing the URL issue.

**Caspar Bowden:** There are two different issues: the website logging issue and then the IP and source port number issue; they are totally different issues.

**David Walker:** I agree with Dr Hosein that it is a curious matter of timing, in that the nature of proxying that has been required with IPv4, which can be used, has an unfortunate side effect, from the point of view of the Committee here, that it often conceals the location or nature of a user. That issue is going to, effectively, go away in the next couple of years with the adoption of IPv6, which will have them for sound commercial reasons.

In terms of the capturing of URL data up to the first slash, it is a very interesting question regarding whether that capture is feasible from the point of view of whether or not that data is concealed cryptographically at the point at which interception is intended or possible to occur, rather than what was said about Wikipedia, for instance. Wikipedia, even though it has cleartext access, is able to identify all the URLs because it would be able to terminate any cryptographic connections to it, whereas if all this information is to be gathered purely by the ISPs, they may be looking just at ciphertext, at which point the data will not be recoverable.

**Trefor Davies:** I would like to add that we would not be able to detect encrypted URL data.

Q1021 **The Chairman:** We understand there are three categories: open messages where you can get everything—the URL and the content; ones where the content may be encrypted but you can get the URL; and ones where the URL and content is fully encrypted and you cannot capture anything. That is, I think, my understanding.

**David Walker:** Yes.

Q1022 **Dr Huppert:** Encryption is something that we recognise is a problem and what you said is very helpful. I am still trying to perhaps pin you down to “yes” or “no” answers, if they are appropriate. If Clause 1 was restricted just to either or both of those specific issues would that, in your view, (a) make the Bill better and (b) make it acceptable?

**Dr Hosein:** You do not need a Bill, in my view. You do not need this Bill in order to do any of that.

Q1023 **Dr Huppert:** But a changed Bill.

**Dr Hosein:** The point I was trying to make was that this data is already collected here, in this country. You could try to pass a piece of legislation requiring foreign providers to record this information, but they are more likely to laugh than to adhere to it.

Q1024 **Dr Huppert:** So the IP data can be done without the legislation and the weblogging, you say, is very hard to do.

**Caspar Bowden:** I think it is legally hard and in terms of human rights it is hard, because if I understand your point correctly, it is about whether we take the premise of Clause 1: that there shall be blanket retention for everybody in the country of certain categories of data. That is still extremely problematic in human rights terms, so I would want to refocus the question on whether the fundamental methodology is collecting data about people about which there is reason to collect—whether there is some basis of suspicion, whether they are in vulnerable groups. To take a rough figure, it is about whether we are talking about 1% of the
Draft Communications Data Bill

population, as opposed to recording data about 100% of the population. That seems to me the essential principle at stake.

_Trefor Davies_: I am not sure that it really does reduce the scope that much. Looking at the original proposal, which is fairly unclear because a lot of it is left deliberately unclear, in my mind, a lot of what might be asked of the ISPs to do is very difficult and it comes down to the encryption and the data being held overseas. If you take away that aspect of it, which is very difficult, you are down to relatively straightforward things, but it becomes about privacy and non-technical debates, because I believe that all of this database will eventually find its way to the public domain and people will be having a play with it.

**Q1025 Dr Huppert:** One of the issues the Home Office has raised is the idea of future-proofing—that the information they need will change in the next few years and a few years after that. There is no doubt technology is changing. Do you accept their argument about the need to future-proof the legislation and what advice would you give us on how to pass legislation practically, if it is required, in this sort of ever-changing world?

_Trefor Davies_: If you are buying into the concept of storing all the information and trying to catch criminals, then it would be a natural thing to provide future-proofing to it. My only technical observation is that people developing applications and services these days are far more conscious of the need to build privacy into their applications and services. You can think of Apple iMessage. Even Skype, for example, is designed to be a private means of communication. I think that future-proofing it as a sort of blanket open book is not necessarily going to have much benefit, because the technical issues are going to be there.

_Dr Hosein_: If I put my academic hat on for a second, there is no such thing as future-proofing. An attempt to make something technology-neutral is a political act. It is an attempt to say that our understanding now is all we will ever understand, regardless of how the environment changes over a period of time. In the first question you heard the answer about IPv4 versus IPv6. That is going to change in two years, so why are we talking about a program over a 10-year period? If we look at, say, the debate we had 12 years ago about RIPA when we were talking about the forms of communications data and how sensitive it is, I would say, arguably, communications data is much more sensitive now than it was back then. We have never had the review debate about RIPA. We are only having it now, unfortunately, 12 years later. If we create a legislative framework that is future-proof it basically means that we will never again debate these matters of principle, and that is very dangerous.

_David Walker_: I agree very much, again, with what Dr Hosein said. If the past and the present are any predictors of the future, it they show that the world changes incredibly rapidly and regarding where we are going to be in 10 years’ time, my professional opinion is I have no clue. Therefore, future-proofing a Bill in this way seems to be a fairly futile thing to go at. The only thing that I would suggest could be done to ensure that the text of the Bill stays relatively current with what the world is doing is that when a Bill relating significantly to technology is passed, rounds of post-legislative scrutiny are put in place and commitments made to do that as part of its passing.

**Q1026 Lord Jones:** I wanted to say, Lord Chairman, thank you to Mr Trefor Davies for his forthright paper, which he submitted in August this year. You say you have a lot of sympathy for those in the area of law enforcement. You went on to say, though, that you have serious
concerns that we are going down a path that might better sit in a George Orwell novel. Have you further to add to that?

*Trefor Davies:* We need to get into the vernacular, then, do we not, in terms of “Big Brother is watching you”? I am not sure that it is a society that we particularly want to live in. Again, it is a difficult one, because I want people to catch crooks. I do not want people to fly planes into the sides of buildings. I think this whole Bill, of all the Bills that we have had in recent years, needs a serious amount of debate, because the judgment and what we come up with at the end has to be based on very informed debate, rather than something that is quickly rushed through because it is perceived that it will provide a benefit, because there clearly are downsides.

I will give you a recent example. It is the first consultation I have ever replied to. I am on the board of the ISP Association and I have always left it to do it, because it has competent professionals to do that. I am not a regulatory person; I am a CTO. But this is the first one I have ever replied to, because I felt strongly enough about the issues. In the course of thinking about it and writing that, for example, I asked taxi drivers. I have had a couple of taxi rides recently, and I said, “Have you ever had anybody leave a laptop in the back of your cab?” I had two taxi drivers who said, “No”, but one of them said that in seven years he had had four laptops left, and one of them said he had had eight laptops left in five years. And then when you read the written submissions about the MoD losing laptops and GCHQ having laptops stolen, it does not matter what security oversight aspects you write into a Bill like this, the information is going to get out in the public domain at some point. I think there will be big downsides in terms of people having their privacy invaded, and you can come up with all sorts of scenarios: somebody might be surfing Alcoholics Anonymous websites or he might have a serious disease that he wants to keep quiet about, or all sorts of personal things. That kind of information will escape. That is really my biggest concern about it.

Q1027 **Lord Jones:** We do read our papers. We are concerned. You mentioned Orwell; why not read *The Road to Wigan Pier* as well?

*Trefor Davies:* I did a long time ago; I have it at home somewhere.

The Chairman: It is because we have all read your papers that you are all here, gentlemen, giving evidence in person.

Q1028 **Mr Brown:** Have any of you given any thought to what elements might be involved in post-legislative scrutiny arrangements were we to recommend such a thing?

*Caspar Bowden:* For RIPA or for any Bill that might come out of this?**Mr Brown:** For this Bill, if there is to be one at all.

*Caspar Bowden:* I have to say that I watched the Interception Commissioner’s evidence with great interest, and I made a number of points about the Interception Commissioner’s role in my written evidence. It seemed to me that the Commissioner’s evidence vindicated a large number of the criticisms that I made. It does not appear to me that the current Commissioner is exercising an effective and credible regime. I do not know what impression he made on you.

I think that I would like to see a much closer connection between Parliament and the oversight and continuous review of any internet surveillance legislation. In particular, in my written evidence, I made reference to a recent European Parliament report that did a
comparative analysis of different countries, how they have set up their oversight machinery and their relationship to Parliament. The UK did particularly poorly in that; the European report was very critical of too close links between the oversight role and the executive. That is indeed the syndrome that we have.

Q1029 Lord Strasburger: Might we get a copy of that European report?
Caspar Bowden: There is a URL provided in my written evidence, but I am happy to point you at it, if you wish.

Q1030 Mr Brown: Chairman, could I just ask if any of the others have anything to add? This is uncharted territory, we know that. Is there anything that any of you could add to that?
Trefor Davies: The oversight aspect of it?
Mr Brown: Post-legislative scrutiny.
The Chairman: If there is nothing to say, that is fine.

Q1031 Lord Strasburger: Mr Bowden has argued for a revamped oversight system with a single unified surveillance commissioner reporting to Parliament. What powers and resources would this new commission need to assure you that the use of the legislation was being properly scrutinised and that the necessity and proportionality of requests was being rigorously tested?
Caspar Bowden: I have done some comparative analysis with the French system and the German system, and there are elements from both that would be worth consideration by this Committee. The French system has essentially a commission. There is no single commissioner with complete authority over that commission. The commission has itself taken on in the past few years, without statutory authority but with the consent of everyone concerned, the approval of communications data access for counter-terrorism cases. It appears to be able to do that with a measure of independence and cost-efficiency, which does not fully satisfy what I would like to see in terms of prior judicial authorisation, but it seems to be much more credible, frankly, than the oversight machinery we have at the moment. They do, for example, emergency authorisation of interception warrants within one hour with independence. They also have arranged 50,000 communication data access authorisations for counterterrorism purposes. They have arranged prior authorisation of each and every one of those. The fully desirable position would be independent judicial authorisation through a magistrate as, for example, now happens with local authorities. I think that could be streamlined and made fairly cost-effective.

Looking at the German system, the G10 Commission is also a mixed commission, and parliamentarians sit on it. I think that there would be room for more stakeholders to be involved. I do question the way in which the Interception and other commissioners are presently constrained to be former senior legal figures. It seems to me there is a case for allowing people at professorial level with a technical background, but also other qualifications and attributes, to occupy that role. Because, frankly, it does not appear to me that at least those figures who get appointed to the role of Interception Commissioner have been able to understand the technical position, if I can put it bluntly. There is simply no evidence in the way they write reports, in the matters they have covered, or in what they have said in evidence that they are in fact au fait with what is technically involved.
Q1032 Michael Ellis: Can we look at the data from overseas, gentlemen? I notice that both Dr Hossein and Mr Bowden have questioned whether overseas CSPs will accept this legislation, because it imposes legal obligations on them and they are outside the jurisdiction. The Home Office has argued that RIPA already does this, and doubtless there are many other provisions on the statute book, some of which have been on there for many years, which also tend to impose obligations on others outside of the jurisdiction. This Bill will simply extend those obligations to the retention of further data. Do you agree with that, Mr Davies?

Trefor Davies: I do not know, other than if I was approached by an overseas government, I would have to be approached via the channels that we have with our own Government.

Q1033 Michael Ellis: Do you think that there will be a problem with organisations outside of the jurisdiction accepting this English legislation?

Trefor Davies: Why would they want to accept it?

Dr Hosein: We have consulted with almost all of the large providers, because the Home Office told us exactly the same thing, which is that foreign CSPs already fall under RIPA, and I was surprised, because I thought I must have been wrong for the past 12 years. When I went to these foreign providers, some of them laughed in response, again, saying, “That is just not true”. And then when we looked into it, the reason the Home Office would say that is because if it was not the case that the foreign CSPs were under RIPA—

The Chairman: I need to suspend. There is a Division in the Commons. We will reconvene as soon as we are quorate with Members of the Commons.

Sitting suspended for a Division in the House.
On resuming—

Q1034 The Chairman: We are back in session again, and back on the record. I would be grateful, Dr Hosein, if you can remember Mr Ellis’ question, if you would start from the beginning in answering it.

Dr Hosein: I do. The Home Office states that foreign service providers fall under RIPA because it has to. Otherwise every request that the Home Office has placed under, say, Google or Facebook would be illegal or beyond the law. The situation for foreign service providers is that they voluntarily reply to some requests. They do not reply to all requests; they reply voluntarily to some requests. Their preference would be that the requests would go through mutual legal assistance treaties, because the challenge they face, particularly those who are based in the United States, is that the standard of law in the United States is far higher than the standard of law in the United Kingdom.

Q1035 Michael Ellis: Are you a lawyer?

Dr Hosein: I am not a lawyer, but I have consulted with all the lawyers I could on this matter. I have consulted with lawyers who are fighting this case in the Supreme Court right now with the National Security Agency and the Bush Administration and the Obama Administration.

Q1036 Michael Ellis: So is it your position, Dr Hosein, that the Home Office is lying?
Dr Hosein: I am not saying they are lying. I am saying that they have to say that in order for their requests to be compliant with RIPA.

Q1037 Michael Ellis: Hold on; I am going to press you on this, because you are effectively saying the Home Office are lying, aren’t you? You are saying that they are saying one thing and mean another thing.

Dr Hosein: I am not saying they are meaning anything else. I am saying that they have to say that in order to be compliant with RIPA with these requests. Otherwise they are making RIPA requests against an organisation that they cannot make requests against.

Q1038 Michael Ellis: There are plenty examples, are there not, of cross-jurisdictional cooperation, not only in this sphere but in many different spheres. For example, the United States frequently imposes obligations, does it not, on other countries that they have to comply with, at least if they want to do business in the United States. Is that not the case?

Dr Hosein: Yes, that is the case.

Q1039 Michael Ellis: It is becoming increasingly common for countries to enact legislation that imposes a burden on other countries. Why do you not see that working in this case?

Dr Hosein: I believe that this Parliament can choose the passage of legislation. I just do not believe that the foreign providers will look upon that favourably or comply.

Q1040 Michael Ellis: Please, gentlemen, you can join in. If the Home Office are saying to the contrary—they are being told something different from what you are being told by providers—what would you say about that?

Dr Hosein: In the discussions we have had with providers they say they respond to requests on a voluntary basis.

Q1041 Michael Ellis: What I am saying is the Home Office’s position is that providers will co-operate with them and therefore they do not envisage this problem that you are concerned about. Do you have any reason to doubt that or refute it?

Dr Hosein: My point is that they voluntarily.

Q1042 The Chairman: Could I pursue this point, Dr Hosein? You said initially that when you took this up with the foreign service providers they just laughed at the concept. Did you find any inconsistency between the views of, say, the London head office of those American providers and the American head office?

Dr Hosein: No, I did not. I did not see any difference between the London office or the foreign offices of these providers.

Q1043 The Chairman: The head office in the States. That is interesting, because I think we were getting suggestions that the evidence we got from our CSPs in the United Kingdom that there would be potential difficulties with this was not the case, because the Home Office had assurances from the HQ in California. Can you cast any light on that?

Dr Hosein: The conversations we have had with senior legal officials in the US is that they want to help—they really do—but the problem, once you start placing legal obligations, is that
if the United Kingdom does it then the Saudi Arabian Government will do it. How do you pick and choose between governments? It creates an awkward environment, so therefore that is why they prefer a voluntary arrangement where they pick and choose which requests they respond to. Secondly, they are far more favourable towards the legal route, the pure legal route, which is compliant with law in the requesting country and the requested country. In the United States, they would like to see it go through the mutual legal assistance treaties that require requests to go through the courts in the United States.

**Q1044 Baroness Cohen of Pimlico:** When we were talking to the Metropolitan Police, it was clear that the biggest of the foreign service providers most certainly picked and chose. For example, they co-operated unhesitatingly if it was murder or terrorism. Certain other forms they refused, if they did not feel that it was particularly appropriate. Obviously our Home Office hope that if this legislation went through, it would stop them picking and choosing, and that they would decide to co-operate fully with whatever request. What would your view be on that?

**Dr Hosein:** My opinion is that we are on a collision course. They are relatively happy with the voluntary regime. The moment there are arduous provisions placed on these companies to do something based on the decision of a parliament in another jurisdiction they are going to start saying, “We will not reply. We will not respond.” That is why I am very surprised that the Home Office is choosing to rock the boat. I do not like the voluntary arrangement at all. I believe in the rule of law. I believe requests must follow some framework established by Parliament, but the Home Office is rocking the boat over this voluntary, slightly dodgy, legal arrangement—or not necessarily strongly bound arrangement.

**Q1045 The Chairman:** Anyone else?

**Caspar Bowden:** I do have slightly different observations to make. I have referred to a problem in my written evidence that I call “schizoid jurisdiction”. This occurs when an international provider decides to respond, say, to a RIPA Part 1, Chapter 2 request or demand for communications data and they fulfil this through their local office and they give this to the local law enforcement agency, exactly as would occur with a domestic communications service provider. But when a data subject—an individual—makes a request to exercise their privacy or data protection rights, then the company will say, “Oh no, I am sorry. That data was transferred to the United States”, and now falls under something like the Safe Harbor Agreement where, in practice, the individual’s rights are much less. So I am a little bit confused by this language of voluntary compliance. I think now all reputable communications providers, whether they are international or domestic, respond to RIPA Part 1, Chapter 2 demands for communications data, so it is not voluntary in that sense. The question that Gus, I think, correctly raised is it is not just the UK that is going to be wanting this. It is going to be Indonesia, it is going to be India, it is going to be regional powers, and all the time there are a few big global providers.

Can I just pursue this and try and break down two aspects in answer to Mr Ellis’s questions? When we talk about the foreign provider complying, what exactly do we mean? Do we mean that they will be keeping data types, which they do not ordinarily keep, in response to some voluntary request from the UK Government? Or, in particular, do we mean that they will be responding to requests to the so-called filter; that somehow they will provide an interface into
their systems, typically in the United States, to allow data mining of very general kinds within their own body of data? It seems to me extraordinarily unlikely that that will occur. Then, to go back to the first question, about whether any international company will retain data types that they would not ordinarily retain, that also seems to me fairly dubious. I would be surprised if any general counsel of a US-based company has given such an assurance to the Home Office. I would find that surprising.

**Q1046 Lord Jones:** Gentlemen, this is on third-party provisions. There has been criticism about this, and I think Dr Hosein has made some criticisms perhaps as recently as July. Some of you have expressed considerable concern about the proposal to ask UK CSPs to collect third party data. The Home Office has not conceded that it might be necessary to write assurances into the legislation, firstly that the original data holder would always be contacted first, and secondly that UK CSPs would not be asked to store or release encrypted data. If these assurances had legislative backing, would they allay your concerns?

**Trefor Davies:** I am not really sure that it makes any difference whether it has legislative backing or not, because the reality is that it is a lot easier for this third-party data to be sourced from the third party rather than from the ISPs themselves. But I would imagine—and I do not have numbers—that a vast proportion of this third party data would be encrypted. Therefore, in order to be able to access it we are into that debate again about the technical feasibility of it. I recognise that in the written evidence there were a lot of different level-playing-field issues and legal and commercial issues, but from my point of view it is the technical practicality of it.

**Dr Hosein:** It is still a form of coercion to tell a foreign provider, “Comply with our request or else your client’s data will be stored by a third party in a foreign jurisdiction”. You are putting the provider in the middle of a rock and a hard place, and that is the intention of this very approach. It is, “Comply with us or we will make sure there is a domestic pool of the data of your users”, and that is highly problematic. I think there is a way through this. It is not for me to recommend policy, but what your question seems to be pointing to is that there are very specific targets that the authorities in this country want to know more information on, whether it is internet places or individuals, and that allows for the type of regime that Mr Bowden talks about, which is a targeted presentation regime, in which you can ask for a national-security-level concern that ISPs in this country would monitor traffic to a specific provider, but in a very specific circumstance, under a very specific authorisation. While there are issues of debate around that, I believe that that is a more proportionate response than going to all the foreign providers and saying, “Do what we say or else”.

**Q1047 The Chairman:** But the Home Office, I think, would say to that point that that is all very well if it is an ongoing operation: you have a potential terrorist, X. “Can we please preserve everything on this guy until we have enough evidence?” That is a different situation from when they come across terrorist Y and then they say, “Can we see what you have?” and we have not been storing anything on him. So you do not provide the whole answer.

**Dr Hosein:** Addressing one slightly different aspect to that, imagine there is a social network for terrorists based in Malaysia—a service provider that runs a social network for terrorists—and we want to be able to monitor all the terrorist activity and terrorist users who may be based in the United Kingdom. There would be a way to have targeted preservation of traffic
going to that specific resource. That is very different from requiring all resources on a “Do what we say or else” regime.

*Caspar Bowden:* I would agree and develop what Dr Hosein has said. I think what we are asking is for law enforcement to look at their task progressively in a different way, which is instead of assuming that somehow there can be blanket recording of this data about the entire population, it is going to be more of a question of beginning, as it were, with the threads that are available and then developing an investigation. You would widen the circle of interest and cumulatively broaden the use of the powers of preservation until you were in a position to acquire the evidence and intelligence you need. This could be something of an upheaval from the way law enforcement has proceeded so far and I think this must be accepted, but honestly, we have to give data preservation a chance. We have to develop a credible regime with which law enforcement can live to try and make this work before we go to the stage of saying that somehow it is acceptable to perform this blanket retention on everybody in the entire country. I will offer, perhaps, a slightly dramatic example of how far we have come in 10 or 15 years. In communist Albania, the secret police, the Sigurimi, used to have a ritual where every year they would require every citizen to come and have a chat with their secret police. Each person would be required to co-operate in building what was called a “Biografi”. This was, as it were, a personal dossier in which they would have to record all of their social relationships, social contacts and main meetings that had happened to them over the previous year. In terms of the way we live our lives now, particularly the way in which social relationships are expressed through the internet, we are effectively allowing the Home Office to build a Biografi on everybody in the country - on their pattern of social relationships and on the fabric of everyday life. It seems to me, just taking a step back, it is extraordinary that we have got to this situation at all and we are even contemplating it.

Q1048 *Craig Whittaker:* Mr Bowden, can you honestly believe for one minute, though, we are talking about an Albania situation here in the UK? We are not talking about building a profile. We are talking about securely storing information. The profile-building, if you will, will be in the access and the safeguards put in place to get that access. I think that is a little bit scaremongering, from that point of view.

*Caspar Bowden:* With respect, not. Look at the testimony of William Binney which I referred to in my written evidence, and his video at a hacker conference in New York which is available online. William Binney was a senior National Security Agency engineer who has now become a whistleblower, objecting to these types of practices conducted in the US. The technology that he, as a senior engineer, was building 10 years ago was in fact precisely an automated Biografi file; it was not merely a question of leaving this data passively in place. And there is a direct correspondence between the sort of machinery that he engineered 10 years ago and what is proposed in the filter. Of course, it depends exactly how the filter is going to be implemented and what lies behind the filter, but I do not think it is correct to imagine that somehow these are, as it were, passive piles of data sitting around. Even if that was the case, there is certainly case law at the European Court of Human Rights to show that blanket retention of this kind of data, particularly if it is going to be used for pattern analysis and traffic analysis, is well beyond what the European Court has tolerated so far.
*Trefor Davies:* Just to add, I think we are kidding ourselves if we think we can keep everything secure. You only have to look at the recent case of the chap who hacked into the Pentagon computers from his back bedroom.

**Q1049 Lord Armstrong of Ilminster:** Changing the subject to the definitions of subscriber data, user data and traffic data—as you might say, the RIPA definitions—the Home Office said, when we saw them the other day, that it might be sensible to reconsider these definitions in order to allay fears that information not traditionally considered as data could be caught by the legislation. What I wonder is whether you think that narrower definitions of communications data or revision of the existing communications data would allay some of your fears about the scope of this Bill?

*Trefor Davies:* Would you care to suggest what the narrower definition is, because I am not sure that I could?

**Lord Armstrong of Ilminster:** We are asking you.

**Q1050 The Chairman:** Perhaps one example may be on subscriber data. At the moment, subscriber data is everything else that remains, which could be, if one was on Facebook, up to about 78 different items. Subscriber data has expanded dramatically since 2000, when it was my name, address and my mobile phone number. Now it could be everything that was on my iPhone, if I had one. That is just one example, possibly, theoretically, where one could say “subscriber data in future will only be X, Y, Z”.

*Caspar Bowden:* I did watch some of the recent evidence sessions where this question was also discussed and particularly the Facebook issue of whether your favourite colour or favourite X, Y, Z could technically qualify as subscriber data. I think it would be a modest and useful restriction to ensure, for example, that that was not possible. However, the way in which we have arrived at the current definitions of the three main categories, it should be borne in mind, goes back to 2000 when RIPA was being debated in the House of Lords and, essentially, the House of Lords lost confidence that the Home Office knew what they were doing, and the definitions of communication data had to be rewritten with some urgency between second reading and report stage.

Industry had some input into that, but I do not think there was much civil liberties input into that, so the definitions we have today have various anomalies. For example, the record of itemised phone calls that one makes outbound from one’s phone currently falls, if one looks at the Code of Practice, into the category of use data, whereas incoming phone calls, which of course the individual does not necessarily see, falls under traffic data, but their impact on privacy is similar. Therefore, I think there would be scope for rationalising the definitions to try to reach some equivalence in their privacy impact, which is the correct way of analysing this, in my view. Most of all, I think one should try and separate the concept of traffic data, in a broad sense, from subscriber data. Subscriber data is essentially static and deals with the identification of people. Traffic data deals with your social relationships, what you are interested in, and what is really going on inside your head. This is intrinsically far more privacy-sensitive and should be dealt with, in my view, much more under the rubric of interception, because the impact on privacy is analogous.

*David Walker:* While I see that clarifying the characterisation of these data types would be extremely useful from a legal perspective, there is a considerable technical problem that these classes of data are very intimately mixed in the communications themselves. To use
Mr Bowden’s example, when it comes to mobile phone calls, the mechanism by which the text messages we are used to sending and receiving on our mobile phones pass from one handset to another uses the same signalling mechanism that is used for ringing someone up. Again, in terms of capturing that data and logging that data, separating them out as part of a capture process is going to be extremely hard, especially given the vast proliferation of protocols in existence.

Q1051 Craig Whittaker: Dr Hosein and Mr Bowden, you have advocated a warrant system, and I think you said it would apply to all agencies wishing to access the comms data. As a Committee, we have heard and taken evidence that the current SPOC scenario and authorising officer system is much more expert and rigorous than a magistrate necessarily would be in a warrant system. Do you accept that might be the case?

Caspar Bowden: In my observation, SPOCs do play a useful role. If one looks again at the current Code of Practice on acquisition of traffic data, the various roles of SPOCs include giving advice and trying to ensure consistency within a particular organisation, and all of that should continue and is necessary. The problem is one of the principle of independence. The authorisation to access this data, as we have covered, can be highly privacy-intrusive—as intrusive, I would say, as interception—and should be done through prior judicial scrutiny. Now, I do not think it is going to work to somehow imagine that one can keep a system that would assign these authorisations to some random magistrate. I think we should consider, together with a reformation of RIPA, how we can organise essentially a specialist magistracy to triage and deal with these in an organised and efficient way and, preferably, to try to put interception of communications also on a basis of prior judicial scrutiny. There would be the opportunity to do two for one, and to have the same sorts of work dealt with by the same sorts of magistrate, but they would obviously be dealing at different levels of justification or suspicion. So to justify interception you would need a more serious and more detailed case than to initiate the preservation of certain sorts of communication data.

Q1052 Lord Armstrong of Ilminster: When you say “interception of communication”, are you referring to the Secretary of State warrant system?

Caspar Bowden: Yes, I am. I am personally not happy with the Secretary of State system for a number of reasons, but I will not digress. I would take the opportunity to consolidate both, ideally. I did notice, re-reading the Code of Practice, that there is a curious self-imposed limitation in the way in which Part 1, Chapter 2 authorisations for communications data are currently applied, which is if a law enforcement agency wants to secure data about the future and to record data, which would not, perhaps, otherwise be recorded, about future communications, the Code of Practice says that can only be done for one month. This is very peculiar. There is no statutory reason or human rights reason why that should be limited to one month. One might think it is almost the Home Office trying to not use preservation very much because they regard retention as such an expedient tool that they do not want to undermine their rationale for justifying the status quo of the retention regime. If one moved to a prospective, targeted, preservation regime, then obviously it would be necessary to authorise the future retention of data for a longer period.
Q1053 Craig Whittaker: Just for clarity then, you are talking mainly about the Secretary of State system. What about a run-of-the-mill SPOC system? I think you were advocating earlier on that we should have a warrant system.

Caspar Bowden: One has to say what one means by a warrant, because at the moment, for interception, a warrant is issued by the Secretary of State. I do not favour that approach. I am talking about a warrant, as it were, issued by a judge or a magistrate.

Q1054 Craig Whittaker: Yes, but I am particularly asking about the system we currently have in place for the accessibility to the data on a much lower level.

Caspar Bowden: As I set out in the written evidence, my own position on this is that provided that subscriber data was limited, in the way the Chairman suggested, to quite narrowly defined types of what we would ordinarily consider subscriber data, I would be content for SPOCs to authorise access to subscriber data. I would say that anything that is traffic data or usage data, which is intrinsically far more privacy-sensitive, should require a magistrate.

Dr Hosein: I am highly sympathetic to the SPOC system as an integrity check and I believe it is a very good stopgap measure for that, but I do not believe it is sufficient for a true test of necessity and proportionality. That is why you need independent oversight. The reason we all like the SPOC system is because the SPOCs are trained. They have knowledge about the technology and about the law. The reason we are currently suspicious of magistrates and judiciary is that we doubt they have the capability. I find that very worrying. If we are concerned that the judges in this country are incapable of understanding the complexity of these types of request, that is something that needs to be fixed beyond the scope of this law.

Q1055 Craig Whittaker: We are not talking about the judges; we are talking about the magistrates.

Dr Hosein: Even so, we would still need to address that issue, because it already exists under the Protection of Freedoms Act that magistrates are involved in some authorisations, particularly from local councils and whatnot. If we believe they lack rigour to respond to these types of requests, how come we authorise them to do so under the Protection of Freedoms Act? I believe that our judiciary and the magistrates may need training at the same level that SPOCs do. SPOCs are a good example of what happens when you train people appropriately.

Q1056 Craig Whittaker: Can I just get you to clarify why you feel that a warrant system needs to be in place above the SPOC system, which appears to be working quite well?

Dr Hosein: The SPOC system may notice errors and may notice some abuses, but the SPOCs look at whether something is lawful. They are not necessarily the arbiters of what is necessary and proportionate in a democratic society. That balancing test between the public interest and individual liberties has always resided with an independent body.

Q1057 Craig Whittaker: Would it help if we put the SPOC on a statutory footing, like we do with those designated senior officers, for example? Do you think that would help the situation?

Dr Hosein: I do not believe it is sufficiently independent. As Mr Bowden was pointing out, communications traffic data is becoming even more sensitive than communications content.
One opportunity for this Committee is to start having a debate about why is it we protect communications content to such a degree but not highly invasive data-minable communications data and why are they any different? I believe once we start having that debate, we will start asking why is it we require a warrant for content but not for communications?

**Q1058 The Chairman:** We are in interesting territory, and I think the Committee generally picked up that the best trained SPOCs are very good and that system seems to be working. The question is about what level of oversight of the SPOCs, and the type of oversight, whether judicial or a commissioner or whatever, is required. That is what the Committee will be agonising over.

**Caspar Bowden:** I just wanted to make the point that looking at the evidence the Committee has received and my own researches over several years—and I do not know what evidence the Committee has received in private—it is still not clear to me what criteria SPOCs use to determine what is necessary and proportionate. Indeed, it is not clear what criteria the Interception Commissioner uses, despite his evidence. If one wants to get down to concrete cases and say for a mugging or for a murder 5,000 people’s data will be accessed, or 50,000 people’s data will be accessed, one needs to have some concrete yardstick of really what is being done, and I have no idea. I do not know if the Committee has managed to unearth that sort of practical information. I noted the Interception Commissioner, in his evidence, said he does not have any difficulty deciding which is which, and I suggest this means that all SPOCs are somehow operating with some sort of magical sense of pre-established harmony, which I find rather hard to believe. I would like to know concretely what is considered necessary and proportionate. I do not think the SPOCs have the independence to really do that in the same way that a magistrate would.

**Q1059 The Chairman:** That is an interesting point, which the Committee will be exploring.

**Trefor Davies:** Just to add, we get RIPA requests, but we do not get very many, maybe one or two a year. By and large, the quality of what we have been asked to do seems to be acceptable and they are genuine right requests. What I did pick up, though, in the written submissions and the written evidence was the Big Brother Watch submission regarding the variations in the way these requests are made. Kent Police, in two years, made 7,664 requests for data with 3,237 of those rejected internally, compared with Merseyside, who made about 30,000 requests and only 500 of them were rejected. It does make me raise an eyebrow a little and ask whether the oversight is really overseeing. The Chairman: That is an interesting question to which I personally do not know the answer at this precise moment.

**Q1060 Baroness Cohen of Pimlico:** Can I just sort out in my mind that Mr Bowden divides subscriber data from traffic data—we all do that—but in terms of subscriber data would be perfectly happy with a SPOC.

**Caspar Bowden:** One has to bear in mind that the Code of Practice does not exclude other interpretations. In fact, I wanted to draw attention to this, as reference was made a couple of evidence sessions ago to the way in which the Code of Practice, shall we say, takes care of these things. If one reads the Code of Practice, it says “the sorts of data falling within this category include”, so the Code of Practice by itself does not exclude far-fetched or over-expansive
interpretation, so I think it is useful and necessary to have very precise definitions in primary legislation that would exclude far-fetched interpretation.

**Q1061 Baroness Cohen of Pimlico:** If we could get the subscriber data definition satisfactory, you would not feel that needed a magistrate. You would be happy with a SPOC doing that. I do not mean to put words in your mouth; I am trying to check.  
**Caspar Bowden:** With other qualifications, that is broadly my position, because I think that represents something that is doable. That would have to be done, in my opinion, with a move towards a preservation methodology by law enforcement.

**Q1062 The Chairman:** Dr Hosein is going to say that is provided someone is second-guessing “necessary and proportionate”.

**Trefor Davies:** Yes.

**Q1063 Baroness Cohen of Pimlico:** That was my next question: even for subscriber data you still feel that.

**Dr Hosein:** I understand that the mood in this discourse has moved that subscriber data is not as valuable, but as a privacy advocate, I have to remind people about the protection of journalists, the protection of journalistic sources, and the protection of leak sources; the revelation of subscriber information will reveal all of that, and so even that needs an independent test of some sort.

**Q1064 Stephen Mosley:** We have heard diametrically opposed views on the filter. On the one hand, I know, Mr Bowden, you have described it as a “hyper-Orwellian menace”, while the Home Office would let us believe it is a way of protecting people’s privacy by eliminating people who they are not interested in. I guess it could be either, depending on how it is used, so the oversight and the control of the filter is going to be incredibly important. What kind of oversight do you think the filter should have to ensure the protection of people’s privacy?

**Caspar Bowden:** Perhaps it will not surprise the Committee to say that I do not think the filter should be built under any circumstances for domestic surveillance. It is understood that GCHQ have had these sorts of capabilities for many years for international communications, but I simply think that the kind of capabilities described in the filter are intrinsically incompatible with a modern democratic society—on the basis of blanket data retention, you understand. If we are talking about preservation of data about designated targets, where for each designated target there is a reason and a justification—even if that is a reasonable belief or a reasonable suspicion—that is still a far smaller amount of data than one would be talking about on the basis of blanket retention. But for anything to do with the so-called filter—I would call it data mining—particularly of traffic data, which is so prejudicial to private and intimate life, I think safeguards and oversight are irrelevant. I just do not think it should be done in a democracy.

**Q1065 The Chairman:** Does anyone else wish to comment?

**Trefor Davies:** I agree.
Q1066 Stephen Mosley: Turning to you, Mr Davies, then, if this filter does come in, a company such as yours will have to interact with the filter and use a standard data format; I know we have been told about RDHI, etc. As a business, would that cause you any problems at all?

Trefor Davies: There is almost certainly going to be an overhead with running and interfacing it, as I am concerned about whether it should be there or not in the first place. 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 it up. I will give you an example: as a business, we are not a small ISP anymore. We have about £40 million turnover, we have a couple of hundred staff and maybe 40 of those people are engineers, but most of the engineers work on day-to-day customer-facing stuff solving problems. The real core of our team who would have to work on this kind of stuff is only six people, and they are network engineers, systems engineers, and applications engineers. We have some deep packet inspection equipment, which we installed two or three years ago to protect our customers’ networks from surges in traffic, and we had to have a couple of engineers working for about three to six months on that full-time, with an external contractor, to install it. For us, there was a business case for doing it.

We have six engineers. 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. It is not a great leap of imagination for me to believe that if I was having to implement the systems to interface with the filter then I am probably looking at half or two-thirds of my development resource, which I then would not be able to have working on my next products, bringing the business into the 21st century with virtualisation and the cloud. Every ISP in the country is racing to try to bring out new products to keep up with the technology, and it really would have a big impact.

Q1067 The Chairman: Are there any outstanding points? I think we have concluded our evidence session, gentlemen, unless you have any other concluding remarks to make.

Dr Hosein: Just one sentence: please do not drop the issue of notification. I will remind you of a case in Poole of the family that was placed under surveillance by the council because of catchment areas. The only way the family was notified of the fact that they were under surveillance was because the council accidentally told them. People need to be informed of when they are placed under surveillance when it is no longer relevant to the investigation or harms any judicial processes.

The Chairman: That is a legitimate point. I have curtailed our discussions today because we are running out of time, but we are grateful to you, in particular, Dr Hosein, for that evidence on notification, which we are considering in written form; thank you for drawing attention to it. Gentlemen, we are very grateful. Thank you very much for coming here today. Thank you for your written submissions initially, which provoked us into bringing you forward to give oral evidence. Thank you very much.
National Policing Improvement Agency [Steve Higgins], Greater Manchester Police [Sir Peter Fahy and Alan Lyon], CEOP [Peter Davies], and PSNI [David Stevenson] (QQ 1068-1140)

Examination of Witnesses

Witnesses: 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, examined.

Q1068 The Chairman: Welcome to the afternoon session. I am sorry we are running slightly late, gentlemen, but you are very welcome here this afternoon. Whilst we all know who you are, I would be very grateful if you would just say who you are and who you represent, for the record, starting with Mr Higgins.

Steve Higgins: Detective Superintendent Steve Higgins. I represent the National Policing Improvement Agency. I also sit on the ACPO Data Communications Group Executive.

Sir Peter Fahy: Peter Fahy, Chief Constable of Greater Manchester Police.

Peter Davies: Peter Davies, Chief Executive Officer of the Child Exploitation and Online Protection Centre.

Alan Lyon: I am Alan Lyon, a Detective Superintendent at Greater Manchester Police and the Senior Responsible Officer for communications data.

David Stevenson: David Stevenson, Police Service of Northern Ireland, SPOC Manager and also the Secretary to the Data Communications Evidence Subgroup.

The Chairman: Excellent. Thank you very much. We have a lot of questions to get through in the time. We will probably run slightly late with you as well. Do not everyone feel you need to answer every single question. If you feel it has been covered by a colleague, then we move on.

Q1069 Dr Huppert: Can I start off with an apology to Mr Davies for not having been with him just before this at another Select Committee, but credit to myself for trying to be in two places at once? The Government has identified two specific types of data that it wants the UK CSPs to retain; it announced this at a session last week. These are data relating to allocation of IP addresses and weblog data—the information up to the first slash. Are you aware of a data gap existing, specifically in these areas, which you think needs to be addressed so that your organisations can perform better?

Sir Peter Fahy: Certainly, as Chief Constable in an area with a serious problem of organised crime in particular, I think the way I would describe this is that often when you are carrying out these sorts of investigations what you are trying to prove is associations. Sometimes this is obviously an association between an offender and a place or an offender and a victim, but often it is associations between different groups of criminals. For instance, if you arrest a foot soldier, in effect, who is delivering drugs and you are trying to prove an association and trying to capture the higher-level drug dealer, then clearly you are trying to prove that association. Up to now, we have been able to use some of the more readily available communication data to do that. But the fact is we are seeing that the criminals are realising that, moving to some of
the new technologies and platforms, and really what we see is obviously, as most people do, an explosion in those new technologies—the new apps—and clearly we are very fearful that we will quickly lose the capability to do that. We already have specific examples of them using some of those new platforms to defeat us.

Q1070 Dr Huppert: Sir Peter, the Home Office said last week that the two main issues were IP addresses and weblog data. Are you saying you disagree: that those two would not resolve it?

Sir Peter Fahy: No, they absolutely would resolve it in terms of starting to capture some of the other forms of communication that we know that those criminals are starting to use. Again—I know you accept this point—it is not about the content of those communications; it is the fact that you are communicating with this other person, which then starts to create the relationship and then we can use other data to prove conspiracy.

Q1071 Dr Huppert: In your experience, do you have a sense as to how important each of those two categories are? Which one covers more of the gap?

Sir Peter Fahy: No, I think they are both equally important and equally responsible in terms of crime investigation and proving that case. But it is fair to say that we are very aware of the way that the technology is developing and therefore, clearly, we need to try and maintain that capability and try to make sure the legislation is framed so that it maintains that capability for the months and years ahead.

Q1072 Dr Huppert: If the legislation were just to specifically restore those two capacities, that then would satisfy the majority of your concerns about the data gap, is that right?

Sir Peter Fahy: I think it would presently. I think we have to be clear, as everybody is, that trying to forecast how technology will develop is very difficult. What is concerning us is that we are continuing to see people offer ways around some of the existing technologies and some of the existing techniques that we use. I want to be realistic with the Committee to say that, clearly, when you look at the way that some of these people are developing, when you see what is being offered—and of course when it is on the net it is available internationally—then I would not want to say that if you provided this and the legislation went through then suddenly the problem would be solved for so many years hence. I do not think anybody could say that.

Dr Huppert: Okay, but it would solve the current one.

Peter Davies: As I know you are aware, we approach this from a slightly different angle. Some of what we deal with at CEOP is serious organised crime. Some of it is more internet-dependent than other bits, but we also deal with protecting children who are vulnerable and at risk, and often the only opportunity to identify them is through communications data. I do not think I can tell you which of the two options you give us are the most prevalent in terms of IP addresses and weblog data. However, I think what needs to be acknowledged is the need not to frame legislation just to meet the needs of today, but to frame legislation that is capable of dealing with the developments in technology of tomorrow. So, from my point of view, our type of offenders—our predatory paedophiles—are online and are among the most sophisticated there are.
Q1073 **The Chairman:** I am sorry, Mr Davies, but how on earth can we frame legislation to meet the needs of tomorrow if we do not have a clue what those things are going to be?

**Peter Davies:** I think the fundamental things about communications data do not change. They are a transfer of data between point A and point B, the opportunity to identify point A and point B, and the opportunity, having done so, to understand what point A, as an account, is doing, provided the legislation enables us to do that. Those are pretty much the same issues to do with comms data.

Q1074 **The Chairman:** With respect, could I disagree on one point? I sat on RIPA in 2000, and in 2000 my mobile phone would give you basic subscriber data, the number I called from and the number I called to. Now my mobile phone tracks me every inch of the way, and every five minutes you have a record of where I am, and that is with most people. That is quite a fundamental change between what you are capable of doing now and what we envisaged in RIPA in 2000. I am merely suggesting to you that to make something future-proof means it is totally open-ended and may be undemocratic.

**Peter Davies:** I appreciate that. I know you will probably explore this in the rest of your questions, but the alternative risk is that you make something that is adequate for the needs of today but does not help people protect the public or investigate the serious organised criminals of two to three years’ time. I am not sure that legislating after the fact on a pretty continual basis, which is what I think would be required to reflect the developments in technology, is a better option.

Q1075 **Dr Huppert:** I understand the point you are making and future-proofing is an issue we have discussed a number of times at this Committee and how one does it and how one ensures parliamentary and democratic oversight, but can I just make sure that I understand in terms of the current problem. As you say, you have a different set of issues that you deal with. Would these two things solve the majority—or the vast majority, ideally—of your current problem as well as Sir Peter’s current problem?

**Peter Davies:** I think they would solve the majority of our current problem, yes.

Q1076 **The Chairman:** Is it the Committee’s view that what you want 99% of the time is who talked to whom, when and, possibly, from where?

**Sir Peter Fahy:** Yes, absolutely. As I say, what is crucial is to be able to prove associations and, in particular, in things like organised crime, to try to be able to capture the people further up the tree so that we are taking out the more serious offenders.

Q1077 **Baroness Cohen of Pimlico:** The other bit of the gap that the Home Office tell us they want to address is data from the overseas CSPs. We understand there are two sides to this problem: some overseas providers do not retain the stuff at all, and some of them do not respond quickly or, indeed, possibly, at all. Can you tell me, all of you, how much of a problem that is, in your experience?

**Sir Peter Fahy:** Again, it is a significant problem, and it is about the two things that you said. It is sometimes the time delay. There are certain providers that are pretty obstructive and are uncooperative. We had a case around Christmas-time where we were up against the custody clock; we have arrested somebody, we are trying to do an investigation, and we are trying to
get enough evidence to get them charged. The international processes are just incredibly, incredibly slow. It is obviously the issue that the internet is international. Often it is not just about us investigating. We then have to do disclosure, so it may be that we have to cover this particular line for the defence as well, and the MLAT procedure, as it is called, we find can be very, very slow. But it is also this issue that some providers are very cooperative, while other providers are essentially obstructive and do not recognise the need. Therefore, clearly, it is important that this legislation, as far as it can, tries to cover that.

Peter Davies: I am backing up what Sir Peter says. This is not an overwhelming problem for us at the moment, but there is every indication, I think, that the ownership of the internet and, therefore, the location of communication service providers, will migrate to other parts of the world. At the moment, where we have good relationships with US service providers and they are subject to some legislation that places an obligation on them to report child sexual exploitation that happens on their networks, the situation is really good or reasonably good. What we need to do is provide for the likelihood that it will not be as good when larger portions of the internet are owned and operated overseas. It is a containable problem at the moment, but there is nothing about it that seems inherently stable, and it may well be a far bigger concern for my centre in the next year or two years.

Q1078 Baroness Cohen of Pimlico: Do you find that the co-operative ones answer all your requests, or do they pick and choose?

Peter Davies: They answer the ones they can, when they can. I think the level of retention and responsiveness is different with each provider. There are some providers that do not have a business need to retain the data, and therefore do not retain it and it is a pretty well articulated fact that roughly 25% of comms data requests currently do not come back with any information. The risk is that that might increase as a proportion quite substantially. I can go on to talk about what that means in practical terms.

Q1079 Baroness Cohen of Pimlico: I am prodding because of your particular field, but we were told by a previous witness that many overseas providers co-operated unhesitatingly if it was murder or terrorism, but for harassment and internet bullying they would not bother.

Peter Davies: We do not deal with harassment or internet bullying. We put people onto those who do. We deal with serious-end sexual exploitation of children by a variety of means. That generally galvanises people.

Steve Higgins: There are two key issues here. One is the speed of the response. We have a system in the UK where automated solutions within the companies for the recovery of the data has significantly improved response times as against a manual process. I think one of the benefits of the Bill, were it to be passed, would be that it would potentially facilitate investment to enable that to take place. That is one of the issues.

The other issue, of course, is that no matter how cooperative an overseas company may be, if they do not have a data retention policy or requirement in place in that particular jurisdiction, no matter whether it is MLAT or any other process, they simply cannot provide us with the information. So it is the ability to work with them and enable the retention of that data.

Q1080 The Chairman: What about their willingness to disclose? I think Mr Davies said there is a 25% nil return. Is that all because they do not have the data? How much of that 25%
is because they may have it but they are not happy to disclose it, because we have not gone through legal means or whatever?

Peter Davies: It is difficult to tell sometimes. It is slower to get disclosure for evidential purposes than for intelligence purposes. That is a distinction. I think almost anything is technically possible if there is sufficient will to do it, and so the issue about what it technically possible crosses over into the issue about what people have the will to do. Each of our relationships with each of the service providers is different. They have different strengths and different areas for development. That is one of the frustrations of what we do, because if there was a consistent level of expectation about retention and access to this data, the extent to which we have to cultivate those individual relationships and, to some extent, hope for the best would be significantly reduced.

Q1081 Craig Whittaker: Just on what you have said there, do you think making retention of third party data over here from overseas, for example, is going to make any difference to that at all? Because we have heard very clear evidence that a lot of companies will encrypt the data, so it will not be able to be used here, so you will still have to approach a company directly overseas yourself using a different method.

Peter Davies: I am not so familiar with what companies will or will not do. I think it depends on what expectation is placed on them by legislation. Let me be clear. The operational ideal, probably for CEOP, but certainly for anybody involved in dealing with serious and organised crime in any of its forms, would be that any level of communications data that is criminal-related within the UK is capable of being researched to the point of identifying the point at which it left to the point at which it arrived and proving the traffic between the two points. I am not so familiar with that issue about third party data, but we would want that to be held within the UK and accessible within the UK, because if that cannot be provided then it is probably lost and, for reasons I mentioned before, that is a significant risk in terms of our ability to use this information to protect people and pursue criminals.

Q1082 The Chairman: You said they might co-operate depending on the legislation imposed on them, but we can pass, in the United Kingdom, legislation that we can impose on British companies or companies operating here. Regarding some of the American giants—and we all know who they are: companies that launched with maybe $100 billion turnover or value and are now a mere $50 billion turnover—why do you think those mega, mega American companies are going to co-operate with UK law, which does not technically and legally apply to them?

Sir Peter Fahy: I think, first, if Parliament passes that legislation it is a pretty strong indication of the will of the country and therefore there has to be a moral obligation upon them. Clearly, all the time we deal with different commercial organisations who sometimes make decisions as to whether to co-operate with policing and with law enforcement or not. We have to cope with that in our day-to-day business and I think it would be absolutely about, sometimes, leveraging public pressure onto some of those organisations, if necessary, to name and shame, to say that, you know, “We feel you should be cooperating and helping us in this form of law enforcement”. In the same way as we might choose to shame a car park operator if they are not taking sensible precautions.
Q1083 **The Chairman:** Do you mean shame companies like Google and Facebook?

**Sir Peter Fahy:** If we need to do that. If it was the sort of serious offending that the public feels very, very strongly about, then I think that we would absolutely need to do that.

Q1084 **Lord Strasburger:** We heard evidence in the previous session that that sort of heavy-handed approach was likely to diminish the voluntary co-operation you are currently getting.

**Sir Peter Fahy:** I think, normally, again, when you are talking to a car park operator or to a major supermarket or to a public house you try and do it through co-operation and, generally, that will work. But I think if you were faced with, as you say, one of these international organisations, which was failing to co-operate and which was not following the legislation, then I think clearly we would be talking to the media and to some of our local and national politicians to make them aware of that, and then clearly they may choose whether or not to apply pressure on them.

Q1085 **The Chairman:** Sir Peter, you said if the United Kingdom Government passes legislation we symbolically show to, say, companies in America we mean business. If Saudi Arabia passed the same sort of legislation, being one of the United States’ major customers, would they not feel under a moral obligation to supply it all to Saudi Arabia or China or any other country that passes a similar law?

**Sir Peter Fahy:** It might well be, but I still think that, on the whole, the sort of issues we are dealing with here and the sort of investigations we are carrying out, there is a very high degree of public concern. I do not believe that some of these commercial companies could ignore that degree of public concern. Clearly, there are issues that, on the face of it, to international companies, may not look that important but which are perhaps leading to serious consequences in this country for individuals, and we know that the public and the media can be very concerned even about individual cases. If it came across, as I say, that a commercial organisation had made it more difficult for us to discover a perpetrator and that had led to a tragedy, then I do not think it would be terribly good for that particular organisation.

Q1086 **The Chairman:** Mr Davies, do you want to come in?

**Peter Davies:** I just wanted to add something. People have been very quick to identify implementation issues or enforcement issues around any of the proposed legislation. There is nothing wrong with that, but those issues in themselves are not sufficient reason not to bother to legislate, particularly in the face of a very clear operational requirement.

Q1087 **Baroness Cohen of Pimlico:** I would like to ask what you all think about the mutual legal assistance treaty process, which is of course the legal alternative—the undoubted, agreed, negotiated legal alternative. How well does that work?

**Peter Davies:** I think it works slowly. It certainly does not work in operational fast time, which is a proportion of the authorities that we require, and I really must hope that I have the opportunity to put a couple of cases to you that illustrate how direct and important some of this information is. 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.

Q1088 Michael Ellis: Chief Constable, I will come to you first of all. First of all, my condolences on the loss of two fine, brave, police officers earlier this year.

Lord Armstrong of Ilminster: Hear, hear.

Michael Ellis: That case I know is active, but there was some reference at the time, at least, in the media, and I think you have made some reference today, to issues within your force area of organised gang activity and that being a serious problem. Would you agree with that?

Sir Peter Fahy: Absolutely.

Q1089 Michael Ellis: Do you have any observations in that context about the value of communications data?

Sir Peter Fahy: I certainly think that, in terms of our current capability, communications data is absolutely vital to some of the successes that we have had, because it comes down to this issue of being able to try to prove associations. It is essentially that if you live in a nice area of Manchester and your house gets broken into and your car gets stolen, you are probably not aware that there is a connection there to organised crime, who are creating the market for that vehicle and probably put the offenders up to committing that crime. At the moment, communications data is absolutely enabling us to identify those sorts of associations.

Q1090 Michael Ellis: So you can prove an association with organised gangs in circumstances where otherwise you might not be able to do so and where such an association is not transparent.

Sir Peter Fahy: Absolutely, because of the way that they are using communications data at the moment. The situation is that when we arrest them and when we charge them they get disclosure through the criminal justice system, they become aware of our tactics, they go to prison, and they sit around all day and discuss, “How did the police capture us this time?” They are aware of the new technologies as really everybody is, but particularly every young person is, and, when they come out, they start exploiting those new technologies. We are starting to see that and that is our concern.

Q1091 Michael Ellis: What sorts of technologies are they starting to exploit?

Sir Peter Fahy: I do not want to go into too many specifics, because I am aware that they are probably listening to me now, but certainly it is essentially particularly some of the new platforms that are available, some of the gaming platforms, and some of the games systems.

Q1092 Michael Ellis: That is what I was going to ask you, about the gaming consoles and platforms. It might not be apparent immediately to everyone, but people can communicate with each other—I will not mention any trade names—from these very common games consoles.

Sir Peter Fahy: As you are playing the games and sometimes you are playing those games on the internet with other people, you can use that to communicate.
Q1093 **Michael Ellis:** Have you seen examples where some of these sophisticated criminal gangs are using those modes of communication?  
**Sir Peter Fahy:** We have, yes.

Q1094 **Michael Ellis:** Would you therefore say that the legislation envisaged by this draft Bill is a vital operational requirement for you in moving forward to defeat these criminal enterprises?  
**Sir Peter Fahy:** Yes, absolutely, I would. It is a vital operation. We are very concerned about the new capabilities that are developing. We are very, very concerned that we will lose some of the ability and some of the capability that we have at the moment.

Q1095 **Michael Ellis:** Chief Constable, has the law kept up so far with the criminal activities?  
**Sir Peter Fahy:** At the moment, it is just about there, but clearly we see it fairly soon losing that. Of course there are issues, absolutely, about our own training, about making sure that we are exploring how new opportunities are covered by that legislation, about talking to the commissioners about that and how that will do so, and about how we create that capability within law enforcement. These are all challenges that we are facing, but absolutely we need the legislation to enable us to do that.

Q1096 **Michael Ellis:** We are at the status quo at the moment, but you would envisage even by the time Parliament takes to pass legislation we need to work to keep up with it.  
**Sir Peter Fahy:** Absolutely. We are seeing this immediately. I was in one of my major investigation rooms this morning. We are seeing this now, so we are seriously concerned that in a short period of time we will start to lose that capability because, as I said, the criminals are very aware of this. They are aware of our tactics and capabilities.  
**David Stevenson:** I just wanted to give you an example of how that has been put into practice. We had an organised crime gang that was using mobile telephony. They were using that to contact a logistics company where they had details of certain consignments. They had those transferred to a different address and made off with the goods. This was national and they did this on several occasions over a six-month period. We were able to identify the mobiles used, worked that the whole way through and eventually it led to very, very little, other than we identified the methodology and the company shut it down so they could not do it anymore. They then transferred onto the internet, where they set up bogus accounts. They set up accounts that were very, very close to legitimate businesses. From those accounts they were able to generate email addresses that looked exactly the same, bar a hyphen, that came from these. So they then got these companies, unfortunately, to transfer these goods somewhere else where they made off with them. Now, we were able to get the IP addresses from the domain name where this was set up. It was set up—they are very, very clever—using stolen credit cards, using wi-fi, using different bits and pieces that we were not able to trace, until eventually we were able to find out that the IP address that logged on to create that domain account initially led back to the leader of the organised crime gang’s house.  
So all we need is to keep the capabilities that we currently have, and I am sure you have been listening to the news today where LTE has landed. That is “long term evolution”, which is 4G. Now, 4G offers data over the internet at very, very fast speeds. It is much, much cheaper than
ordinary telephony. What we have at the minute is a situation where, if communication service providers are keeping this data for business purposes, we can get access to that. If they no longer have a business need to keep this data, if they offer an “all you can eat” tariff for everything, they will not need to keep any of this data, and this legislation is to try and protect what we currently have.

Peter Davies: I agree with what has been said. I just picked up that people might have the impression that everything is fine about the current arrangements. This is not to diminish the importance of future-proofing, and the arrival of 4G is a great example, but everything is not fine about what we currently have. If you are using high-volume data inquiries to investigate an organised crime group in relatively slow time, a 75% hit rate may be adequate. If one piece of communications data is the difference between life or death, or serious harm to a child or not, then leaving it to three out of four is not adequate. I would like to mention three cases very briefly that I think it is really important that I have the chance to mention, if I may. These are cases from within the last eight weeks in CEOP.

First, the good news: a contact between a child and a helpline service online, where the child indicated that they had self-harmed and were intending to commit suicide. Following normal procedure, this was passed on to CEOP as the agency that tries to reconcile the IP address to an individual. We did so in a very short space of time. We passed it on to the local police force in a very short space of time. They responded in a very short space of time and when they got into the address where we located this person, the child had already hanged himself, but was still breathing. Now, if there had been any delay in that process or if the child had been unlucky enough to be using one of the service providers that does not come up to the three out of four mark, that child would now be dead, and I do not think there is any level of tolerance or acceptance that that might have had a different outcome.

There are two other examples where we do not know what happened. I do not normally use these words, but I think it is important to convey this: there was somebody using a paedophilic chat room called “Child rape torture brutality”. That is the name of the chat room. An individual had been on there once recently and once previously, and, quite simply, we were unable to identify this individual because the communications service provider does not record the IP subscriber information. I am sure you would expect me or any one of the 100,000-plus police officers, if we knew who was going onto this site, to do something to investigate and mitigate the risk they present to the public, but this was one of those occasions when we could not. I do not know who that person is, which is why I am not afraid to share that with you.

One more example, from this month: somebody offered online, for distribution, a number of indecent images of children, including files indicating the rape of a female four-year-old. We were unable to identify the suspect, because the comms service provider does not record the IP subscriber information and there were no other lines of inquiry.

Ladies and gents, I think it is really important to acknowledge that the communications data retention, accessibility and availability is the difference, in some of our cases, between children coming to serious harm or not, and I am grateful to have had the opportunity to convey those recent cases to you.

Q1097 The Chairman: In all of those cases, it is IP addresses that were the missing ingredient, not everything else in Clause 1.
Peter Davies: Yes.

Q1098 Michael Ellis: Mr Davies, if I may say so through you, Lord Chairman, you in child exploitation and your officers do a very difficult job and one that is very much appreciated. Thank you for enlightening us about those examples. I take it from that that you would wish to emphasise that it is not just a question of the status quo, retaining abilities that law enforcement currently have. We need to move in line with advances in criminal activities and therefore enact measures that will help law enforcement deal with these issues.

Peter Davies: Absolutely, and my point is that the status quo, while tolerable in most circumstances, I do not feel is tolerable in the circumstances I have described.

Q1099 Dr Huppert: Sir Peter, you were talking and following, I have to say, very nicely the Home Secretary’s line about games and other online activities like that, and how legislation was needed because people talk on games. Can you tell me which bit of RIPA does not apply to that already?

Sir Peter Fahy: It is not about RIPA. It is, exactly as Mr Davies described, about the fact that the organisations that are providing this capability have retained the data, so that we can identify who the people are who are using it.

Q1100 Dr Huppert: Are you saying that the whole issue about whether it is online games and the fact that people do all sorts of things like that is a complete red herring? It is about whether you have the IP address data.

Sir Peter Fahy: Yes, absolutely. It is about whether that provider has retained that data and we can get into it.

Q1101 Dr Huppert: So you would advise the Home Secretary to talk about IP data rather than online gaming as a particular issue.

Sir Peter Fahy: We are just trying to give—and I probably think she drew it from me rather than me draw it from her, but clearly we have been talking to the Home Office about what we are seeing in terms of the methods that criminals are using. We have used that as an example, but I would not want to limit it to that. What we are seeing, as I say, is a huge development of apps and of different offerings from different providers, and some of it feels certainly that it is only designed as a means of getting around law enforcement. Some of it is also to get around not being charged. There are services where essentially you can get a phone number and a means of communication that essentially means you are no longer paying a mobile phone bill. It is that sort of thing that we are concerned about, which is developing.

Q1102 Craig Whittaker: Can I just ask a question for absolute clarity? One would presume that because you know about these apps and you know about the gaming scenario, that if you need that information you can approach these companies and get the information going forward. The issue, I presume, is about what has happened; is that right?

Sir Peter Fahy: It is clearly whether that company chooses to retain that data.

Q1103 Craig Whittaker: But you can still request them going forward to retain that data for a period of time, so that they could help with your inquiry. I know it is not going to help in a
life-and-death situation, but for serious crime, which is what you are talking about, it is about what has happened, rather than what is going on at present.

Sir Peter Fahy: Yes, that is right, but I would agree with what Mr Davies said. Clearly, even in terms of our current capabilities, there are a lot of frustrations, because again, if you are talking about mobile telephony, the criminals will do everything they can to make it more difficult to identify who has what phone. But that is a separate issue.

Q1104 Lord Strasburger: Mr Stevenson, can we go back to the example that you gave us, which was a very interesting one. Presumably, that was an ongoing investigation where you had identified suspects.

David Stevenson: Yes.

Q1105 Lord Strasburger: Surely intercept evidence would have given you everything you needed, and far more than you would get out of communications data.

David Stevenson: My knowledge of that is very, very limited. That is a completely different area and I would not be able to speak about it.

Q1106 Lord Strasburger: My understanding is that this is exactly the sort of case where you would go to intercept, with a warrant, and you would get all the information you want and more that way.

David Stevenson: Again, I am unable to speak about that specifically. However, if the Lord Chairman wants, certain evidence can be given in a written form.

Q1107 The Chairman: Yes, we will ask briefly on that, because it did strike me as well that probably going to the Secretary of State’s warrant in Northern Ireland to get intercept evidence when you have known suspects may have been a route. It may have been used and you are not aware of it, in any case, at your rank, Mr Stevenson.

Sir Peter Fahy: We would have to say that the criteria for getting intercept from a Home Secretary’s signature is extremely, extremely high and therefore we would not normally think about it in a case that involved the theft of property in this way.

Steve Higgins: I have just a brief point. The focus has been very much on serious and organised crime, and I completely understand that and support everything that has been said. There is another facet to this that may be worthy of note, which is the unwitting. A lot of these technologies are now used as a matter of fashion, rather than a deliberate attempt at subterfuge and I think that is a key point to bear in mind. In policing, clearly our primary focus is about saving life, followed by the prevention and detection of crime. The issue is that, certainly for the general public, a lot of their key concerns are about volume crime and in these areas where you have unwitting use of technology that does frustrate, that is a problem. To come back to the point that you made about the other alternatives that are open to us, clearly in those cases that would not be an option.

Q1108 The Chairman: DCI Higgins, a lot of these things you say may be fashion and there is a problem for the police in keeping up with it. We have had evidence from witnesses in the past who have said that a large part of this problem could be solved by better police training or better SPOC training, so they can know what they are asking for from the huge amount of
Steve Higgins: I think there are probably a number of questions sitting under that one, Lord Chairman, so I will perhaps try and address them in order.

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. We have approached that over the last two years in a number of ways. Specifically in relation to SPOCs, we introduced a programme to refresh the knowledge of every accredited SPOC in the country. That was in the form of a three-day course that was rolled out. We are currently looking at the accreditation of SPOCs and reviewing that, and looking to introduce a programme of continued professional development, applying a framework of information, so moving away from perhaps the old approach of a single course and then a number of ad hoc attendances at seminars, through to a more consistent national standard in that regard.

If I move on to investigators and analysts, again there was a significant gap that was identified in relation to this. The way that we have approached that is we introduced a five-day course, which is the Core Skills in Communications Data course. That has now been rolled out, since October 2010, to over 5,000 police officers and staff. The follow-on from that is that we are now looking to embed that training within existing programmes of training that are rolled out to trainee detectives within the Professionalising Investigation Programme, which is a national programme run by the NPIA. In this way, the standard that we sought to bring detectives up to two years ago or a year ago, is now embedded within new-to-role training. We are looking now specifically at more specialised areas of training and so, in relation to analysts, we have just rolled out a six-day classroom-based course for specifically targeting analysts in the use and exploitation of communications data. We have also rolled out a specialist course for radio frequency technicians. We are currently looking at the possibility of rolling out dedicated training for a more limited number of detectives who are specifically involved in the more high-profile, complex and serious investigation of crime.

Q1109 The Chairman: What training do you do on advising SPOCs and officers on what is necessary and proportionate?

Steve Higgins: Clearly, that is a key part of their role, so part of their responsibility is to act as guardian and gatekeeper, as outlined in the Code of Practice. They are there to provide independent advice and judgment, if you like, both for the applicant and for the designated person who authorises the application process. They are taught very much to understand the difference between proportionality and necessity, and that a key part of the role is to scrutinise the applications that they receive. If I look at proportionality, it is about the level of intrusion into someone’s privacy and whether that is balanced against the benefit to the investigation of that data. Necessity is about linking up the links between a mobile device, a crime scene and, potentially, a witness or suspect.

Q1110 The Chairman: We are aware of the filter arrangements—the RHID scheme—being developed. If, for the filter to work, there is a standardised Home Office-run set of questions
or a program or format, do you then see less role for training SPOCs, if it is all going through a big centralised Home Office filter system?

**Steve Higgins:** No, I am afraid I do not, Lord Chairman. I think there is a basic requirement—and this has been reiterated by SPOCs such as Dave, who have been through the course and are very experienced now—for all SPOCs to understand the legislation, the application of that legislation within an investigative process, the network operations—so how networks operate and function—and also the data that is available to them. That is a basic requirement. I think the arrangements that you refer to that are set out within the Bill will help in certain circumstances potentially to reduce the burden on SPOCs. Again, it has been identified as a key challenge as more and more data becomes available and the thirst for data and information increases, not only to convict; investigation is about proving guilt and innocence, so it is about corroborating alibis as much as it is attempting to prosecute. I think the importance there is that potentially that will reduce the burden on the SPOC and the SPOC unit, but that will, in turn, free up their time, so that they can provide the advice and support that they are there to give to investigative teams.

Q1111 **Lord Strasburger:** Do you have any training material on necessity and proportionality that you would be happy to share with the Committee?

**Steve Higgins:** I would be more than happy to share any training material or, indeed, if the Committee was minded, I am quite happy to facilitate a brief demonstration of a mixture of the training that is provided.

**Lord Strasburger:** I think we have missed the slot on that one, but the material would be useful.

Q1112 **Dr Huppert:** The training is clearly very important and the test around proportionality is really hard and it assumes that there is a reasonable way of judging that. You will know, presumably, that Derbyshire Chief Constable Mick Creedon, who runs Derbyshire Police and speaks on serious organised crime for ACPO, said about proportionality, “If I am driving on the motorway and I see someone on a phone and texting at 80 miles an hour, that, for me, would pass the test”—of proportionality—“immediately”. Would you agree, in the absence of any other information, with the chief constable?

**Steve Higgins:** I think it would be inappropriate to comment with the absence of any other information. I think it is key to recognise that each case is considered on its merits.

Q1113 **Dr Huppert:** But he said given just that information that would pass the test. I realise that he is a slightly higher rank, but would you be training your SPOCs to reject an application from a chief constable? If not, are you not concerned that another chief constable may come in with something like that?

**Steve Higgins:** Absolutely, we do train our SPOCs to accept the position that they may well have to challenge upwards and that is part of their job; I think that is accepted.

Q1114 **Dr Huppert:** So you train your SPOCs that if they got a request like that they would say it was or was not proportionate.

**Steve Higgins:** As I say, I am not going to be drawn on a specific case without further information.
Sir Peter Fahy: I would be expecting them to ask, again, what the context is, whether there was a problem with fatalities on that particular stretch of motorway, or whether there were other circumstances.

Dr Huppert: And if there were no other circumstances?

Sir Peter Fahy: Again, I think what we are showing is that—

Q1115 The Chairman: We are getting a bit hypothetical now and into chief inspectors challenging chief constables, but Mr Davies wanted to comment.

Peter Davies: Which, if I may say so, in the context of RIPA, they are welcome to do and those are part of the rules. I know you know what I am going to say. I do not recall Mr Creedon saying that. I know it was attributed to him following a press conference, which I also spoke at. I do not remember him saying that at the time.

Following the last Committee appearance, I checked with him whether he had said that, because I must admit I would have been mildly surprised if he had. He said my recollection of what he said was accurate, which was that if you are investigating a fatal road traffic collision on a motorway, it is of evidential relevance whether somebody may have distracted themselves at the time of being involved in the collision by, for example, making a telephone call or texting. I think that would be proportionate. I think that is what I heard him say at the time and that is what he recalls having said subsequently.

Q1116 The Chairman: I have a completely different recollection, because I sat there at the time as well, but we will not debate that today and we will probably not be using it in our report.

Alan Lyon: I think it may be important at this juncture just to highlight the issue that not only is it important to train our SPOCs sufficiently, but also it would be helpful, I think, for the Committee to understand just where they are located and their relationship to their colleagues. They are very much separated from the investigative team and they work in a very confidential environment. They are vetted to an enhanced level, and access and control to those members of staff working in that suite is very strictly controlled. So they do take their role as gatekeepers and challengers of senior officers, where it is appropriate, very, very seriously. I, as the senior responsible officer, do support them in that. It is a very, very important and key role for which they are properly trained, as my colleague has just outlined, but that is also a continuous professional development programme of regular training attendance. Of course, we are still under the scrutiny of IOCCO.

Q1117 The Chairman: That is okay. I think the Committee has seen sufficient evidence that we are reasonably assured that they are not just rubber-stamping the requests of their pals. We realise that. A final question from me on this is: would you put the SPOC system on a statutory footing on the face of the Bill, the same as the Authorising Officer?

Alan Lyon: I am not quite sure whether there is a need. We have talked about necessity and proportionality. I am not convinced there is a need at this stage to do that and to be specific, as in the Authorising Officer’s role. For me, my experience of the SPOCs—the way that they fulfil their duties, the way that they protect a very sensitive tactic and do it in a very responsible manner—does not give me cause within Greater Manchester for the need to do that.
Q1118 The Chairman: There may not be a need. Do you think it would give public reassurance?

*Alan Lyon:* There are perhaps other ways of giving public reassurance. 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.

Q1119 The Chairman: Could that inspection process be beefed up a little bit?

*Alan Lyon:* Again, the inspection process is at the discretion of the independent panel, the Interception Commissioner, and if there was any concern about our handling of such a tactic they would inspect us more rigorously and more frequently than they do. I do find that the IOCCO process is robust. Incidentally, our inspection takes place on Monday. The inspectors will be with us for three days and they will explore a broad spectrum of our work, from serious organised down to divisional crime, level two criminality, that we investigate and apply the tactic to. So it is very robust and they will be speaking not only to the SPOCs, but also to investigators and applicants and every tier of the process.

*Sir Peter Fahy:* I personally think it would be of benefit if the public perhaps understood a bit more about how seriously we do take this issue. I have certainly seen it in counterterrorist cases where the view is seems to be that the police can go around tapping everybody’s phone, which is clearly not the case. We have put a huge amount of care into this, there is a huge amount of recording of data and, yes, I think sometimes it is frustrating.

Q1120 Michael Ellis: There is a lot of misinformation.

*Sir Peter Fahy:* Absolutely. 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. My people know that I treat this very, very seriously because it is a very, very valuable tactic and if there was any cause for public concern that this was being abused, as I say, it would be very damaging to the police service and, probably more importantly, very damaging to the investigation of crime and protection of victims.

*Peter Davies:* Notwithstanding what Sir Peter and Mr Lyon have just said, the only other thing I would comment is, having tracked this debate for quite some time, if we had the choice between a beefing-up, through legislation, of the existing process of authorisation, transparency and accountability, I would regard that as preferable to the replacement of it with something entirely different, which was one of the ideas in circulation at the time of the last Committee and prior to that.

Q1121 The Chairman: You used my phrase “beefing up”; what is the beef?

*Peter Davies:* I was using the term “beefing up” in, I think, the same way as you were trying to use it, which is enhancing a system that is already there to provide a greater level of transparency and accountability, if that is required.
Q1122 Lord Strasburger: We have received evidence that the Interception of Communications Commissioner or a new body should have a more public role in reassuring the public that communications data is being used responsibly. How often are external checks presently carried out and what does the checking consist of?

Sir Peter Fahy: I would certainly, from my point of view, as I have indicated, welcome absolutely more public reassurance. Clearly, what we would not want is that to get into the description of some of the tactics that are being used, but I think it will possibly be something we want to discuss with the police and crime commissioners when they are elected later next month. So, absolutely, as I say, I have some frustrations: I would like the degree of seriousness that we treat this area in possibly to be better reflected with the public. I think you have heard we have a very rigorous inspection regime. We treat that very seriously and, to some extent, of course that is monitored week by week, because again certain of the RIPA authorities have to go to the commissioners and, if they do not approve of them or think the ones that we have approved were inappropriate, they will tell us very rapidly. So there is already the inspection regime, but, as I say, there is almost the daily monitoring of authorities and RIPA authorities and feedback coming back as to, “We agreed with that one” or “We did not agree with that one”.

Q1123 Lord Strasburger: The Interception of Communications Commissioner’s report for 2011 showed that they had carried out 22 fewer inspections of police forces in that year than there were police forces. So I can deduce from that that 22 police forces did not get inspected that year and, presumably, then went two years without an inspection. How frequently is your force inspected?

Alan Lyon: It is at the discretion of the commissioner. We were last inspected in September 2010 and, again, at their discretion, they are now due to visit us in November 2012. And for me, when we debrief the report on their findings and, indeed, brief the chief, we look at their recommendations, we look at their advice. In fact, since their last inspection process we have streamlined some application processes, because they found us being too challenging to our applicants. We have taken that advice onboard and have worked together collaboratively to reduce the number of applications and streamline them when appropriate, and that is fully within the legislation and fully within their guidelines. I think the very fact that they are coming back from 2010 into 2012 indicates a degree of confidence and satisfaction in their findings during that inspection.

Q1124 Lord Strasburger: Sir Peter, I think you were saying that you would be comfortable if the inspections were at least annual, to give the public more reassurance. That is what I understood you to say.

Sir Peter Fahy: It is really about the way that that is communicated. Essentially, if there was an inspection every year, but the public were unaware, then it would not be serving a great deal. I think there is an issue about how we communicate to the public the seriousness with which we treat this area. As I say, at the moment, when there are particular community concerns perhaps about a particular investigation, and often it is in the counterterrorist world, I think we certainly, at that stage, feel that some of the public and even some people who appear to be well informed do not actually understand how seriously we take it. But I would come back to: there is almost a daily interaction and we have had a particular type of authority
where essentially the commissioners did not agree with us, and we had a fairly open conversation about it, but at the end of the day that was their decision. So it is a constant relationship in terms of how seriously they take it.

Q1125 Lord Strasburger: Are there any other changes any of you would like to see to the existing system?

Steve Higgins: Perhaps something to add, looking at inspection regimes, but maybe something worth pointing out is that the process by which we apply communications data is subject to routine scrutiny, because it is all subject to the CPIA. There is a requirement upon us to disclose that process through the courts. I requested just a brief review through the Metropolitan Police prosecution support team and asked them whether they were aware of any adverse court decisions on the basis of an abuse or a breach of that process, and they were not aware of any.

Q1126 Lord Faulks: Sir Peter, we have an independent reviewer of terrorism legislation. Do I understand what you are saying is that you would really like the equivalent publicity and priority and prominence to be given to those—such as the Information Commissioner—who are monitoring what you do, so the public gets an idea that there is someone independent on the case and reassuring them?

Sir Peter Fahy: I would be very, very clear that policing has always benefited from greater transparency and accountability, and I would be very, very clear about that as long as there is nothing that, perhaps by slowing things down, makes things more difficult. What I think is always interesting as well is we inspect on the basis of almost whether we have abused this legislation. We are never really inspected on “Are you making best use of this legislation?” And to be fair, I have had some commissioners who have said to me, “We think you could do more of this. We do not think we are getting enough applications from your force”—it was from a different force that I was in.

I think we have made it clear that we are trying to keep up with the training requirement, but I think, as every organisation, when you see the way this capability is growing, we absolutely do have a challenge in terms of training our staff, making sure we recruit the right staff to absolutely understand the capability, understand the legislation if we are going to keep up to that. Therefore, absolutely independent people who can help put some challenge to that are important; for instance, we in Greater Manchester are talking to our universities about whether they can help us in this area around research and capability and those sorts of things. But the general point I would make, as I say, is that policing has never had anything to fear from greater accountability and transparency. If that reassures the public that we are using this properly and that enables us to use the capability to then protect victims of crime, that essentially has to be a win-win for everybody.

Q1127 The Chairman: Are you aware, Sir Peter, of any forces who may be employing, next to the SPOCs, people who may be called “computer geeks”, who may not have been recruited initially for their police constable abilities, but have a knowledge of what to look for and what to ask for?

Sir Peter Fahy: We are increasingly trying to do that. Part of my reflection almost is that I need to recruit a room full of 14-year-olds to do this sort of thing, but there is a serious point
Q1128 Baroness Cohen of Pimlico: I think some of us who visited the Metropolitan Police formed a very favourable impression of the whole SPOC process. I think what we are trying to address is whether there is a better way not of doing it, but of getting it known that this Bill could be deployed to use. That is why we are asking whether the system could be made legally enforceable, because that would be infinitely reassuring to quite a lot of the general public.

Sir Peter Fahy: As a Chief Constable and from ACPO, clearly we now have a lot of defined roles in policing in terms of all sort of high risk areas, like firearms, counterterrorism, and even the investigation of murders. For instance, you have to be a senior investigating officer to investigate a murder; you have to have a record of achievement, all those sorts of things. We do not specify that in legislation, but it is absolutely there as what we now call “approved professional practice”, which will now be signed off by the new College of Policing. I think we recognise that there is a need to show the public that we are professionalising policing and that absolutely there are key roles that we treat very seriously and are common across all forces.

Really, overall, that is the way that we would like to approach that probably, rather than just picking out particular roles because, as I say, the public should be equally concerned that the people who, for instance, are in charge of firearms operations themselves are trained to a certain level and it is treated very seriously. I think there would be a difficulty if we started to define all those different roles in legislation. It is rather about saying we take all these things very seriously in high risk activity. It is now in the new strategic policing requirement, which again has been approved by Parliament, and, as I say, will then go into an accreditation scheme in the new college of policing.

Q1129 The Chairman: On the other hand, we do not want deep public concern and thousands and thousands of people worried about how you investigate murder, and we do not have specific legislation on that. We are facing specific legislation here on a technical area where there is deep, deep public concern at the moment.

Sir Peter Fahy: Yes, indeed, and I think, as I have said, anything that would perhaps reassure the public and that would increase that transparency and accountability, we would not argue about.

Q1130 Lord Armstrong of Ilminster: I wonder if you would see any merit in creating a team of highly experienced and trained what you might call “super-SPOCs”, who could provide oversight and advice. I am not suggesting that the Met or Greater Manchester necessarily need it, but it might be useful across forces, particularly for those police forces that only have occasional access.

Sir Peter Fahy: We recognise that in organisations like the NPIA and the Metropolitan Police, and even in CEOP, there is already a foundation of expertise. And again, the idea is that as we develop particularly the College of Policing, we absolutely would like to have the idea around
SPOCs and that expertise about this area within there. To a degree, we have that at the moment. You saw that in the case in Wales; when we have a particularly complex search you can go to various experts around the country who will help you, as a police force, in carrying out that search. I think your suggestion is a good one: that, essentially, in this sort of area there should be a group of experts identified that a particular force would want to go to. I think I have also expressed the concern I have that we need to build this capability for law enforcement, and we will be talking to the Home Office about, in the new world of the National Crime Agency and the College of Policing and other developments, where we will, as a country, be developing that capability around our understanding of communications data and the way that crime is going onto the internet in general. I would identify that, as a country, we need to build that capability. But particularly, as I say, around that area of expertise—around SPOCs and this particular area—I would like to see that developed within the new College of Policing, as a community of good practice that an individual force could approach if they wanted advice about a particular issue.

Q1131 Lord Armstrong of Ilminster: I am encouraged by that answer, Sir Peter. I wonder if I could ask a more general question, which you may not want to answer; I do not know. There is a scheme whereby local authorities who are minded to use communications data for investigations can use the services of the National Anti-Fraud Network. They do not have to, but they can use experienced SPOCs in the National Anti-Fraud Network and the evidence we have received suggests that the experienced SPOCs in that network do a very good job. I wonder if you think that it might be sensible to widen that service, so that all the public authorities that use communications data only occasionally had to put their requests through a centralised SPOC service, so that we got the level of experience and training and common practices and standards in relation to necessity and proportionality.

Sir Peter Fahy: I think, in general, we would support that. I think our concern has been that obviously sometimes the reported use of this type of legislation by certain other authorities has created the danger of calling it into disrepute. I think that is a risk for us in law enforcement in general, if the public and the media feel that some of that legislation, which they believed was intended for more serious forms of crime, was used for activities that the public themselves would not see as serious. That greater national oversight of that is something we would welcome.

Q1132 Lord Armstrong of Ilminster: Mr Davies, do you want to add to that at all? Peter Davies: I just want to endorse that. I think most police forces use this kind of authority process fairly frequently. Practice may not make perfect, but it makes far closer to perfect. If it used rarely, then there will not be the expertise, and provided that expertise is provided from somewhere, through a scheme such as the one you describe, that has to be better than leaving it to people getting to grips with these kinds of powers, so I endorse what Sir Peter says.

Q1133 The Chairman: On bringing things into disrepute, you and many other witnesses have said and the Home Office in public session last week, “What we really need are IP addresses and weblogs”. You and others have said, “We are really interested in who, when and possibly from what location”; that is pretty narrow. We have had witnesses who have
said, “If that is all the Government wants, it is totally unfair to designate this Bill as a snooper’s charter. But if Clause 1 stands as it does at the moment, then it is fair to designate it as a snooper’s charter.” How concerned are you that we have possibly got a draft Bill, which has been brought into disrepute because the Home Office have phrased Clause 1 so widely that, theoretically, everything could be caught. There has been inadequate consultation on it and yet, as we get further and further into our inquiry, it seems that what they want and what you want are much narrower things than Clause 1 designates. My question is: have the Home Office made a rod for their own back in making Clause 1 so wide, because it does not seem to be what you need?

Sir Peter Fahy: We were obviously very, very concerned about some of the initial publicity and some of the public debate about this proposed Bill and some of the earlier forms of this Bill. We felt some of that debate was very, very ill-informed and did not take into account the nature of crime as we see it, the nature of organised crime, and the reality of the tactics that the criminals are using. Of course, again, chief constables, on the whole, were wary about getting into that debate, because it was becoming party-political and we are very wary of getting into that space, particularly after certain experiences we have had in the past. Unfortunately, that created a lot of information that this is now playing into and it feels like a bit of a catch-up to try and get across how serious this is.

In terms of the way the Bill is formed, we have certainly tried to express that it is trying to get the balance about absolutely reassuring the public and getting the balance with civil liberties right, but on the other hand, trying to make it broad enough to capture what might be future developments, so that we do not have to keep on coming back to this area.

Peter Davies: I will skirt around some of the observations you might be inviting me to make about how the Bill was formed, and so on. I think where I find my limits is in expressing the operational requirement for this kind of data to be captured, accessible and available in quick time, when necessary, to a whole variety of agencies whose business it is to enforce the law and protect the public. Whether Clause 1 overextends what is necessary, and it may well, that has to be a judgment for legislators, in my view. I think there may be some aspects of what is included that are more essential than others, but here is the thing: we are not legislators. We are here to express an operational requirement for data. So I am not sure I can answer the fullness of that question, but we understand entirely the need for accountability. We understand the relationship between possibly future-proofing this legislation and creating too much freedom and flexibility. I do not regard myself as an expert on how to navigate that, frankly. What I can say most clearly is that we look to you and the legislators to navigate that on behalf of the public, so that the right balance between the need to protect the public from harm and protect the public’s right to privacy is struck. I am not the person who will advise you how to do that.

Sir Peter Fahy: The only other observation I would make from my experience is, overall, what has benefited this country and law enforcement is that we have been given the capability to use certain powers and certain capabilities that are sometimes denied in other countries. However, what has controlled that has been the level of oversight and inspection and regulation around that and the attitude that the courts take towards that. I personally think that is the right balance. You go to other countries where, for instance, there is no CCTV and the public would not trust the police with CCTV, whereas I think in this country we have that facility, it is there available for the public, but we treat it very seriously and control it very
seriously. For me, that is the right balance. That is why, we would say, we would absolutely welcome any form of oversight or inspection if that reassures the public. That reassures them that the police are being properly overseen and regulated and then, as I have said, the victims of crime and those who may be victims of crime are getting the protection. I think the worst of all worlds is when society does not trust the police and does not give them the powers and capabilities, and it is the victims of crime who then lose out, and you do see that in some countries.

Q1134 Michael Ellis: Further to the point you made—I am not going to invite you to make politically loaded remarks; far from it—would you say that the media coverage has, in places, certainly in the early stages of this matter, been a travesty of the truth. Certainly regarding talk of the Home Secretary being able to read people’s shopping lists and the content of email, a lot of that was grossly misinformed. That is not a political point; that is simply an accurate reflection of the difference between what the draft Bill says and what was being reported. Would you agree, Sir Peter?

Sir Peter Fahy: I would agree with that and, obviously, I do see it from a certain point of view, as somebody who sees the consequences of serious and organised crime in communities and the way that blights the lives of people and destroys the aspirations of young people. I have that particular view of it, and in some of the comments I just did not recognise that people saw the reality of what it is that we are dealing with and the threat that it poses. I would also say that another break we have is the resources one. I do not have the resources to go on fishing expeditions through people’s shopping lists. Every day, we have to look very, very carefully at a huge number of threats and consider where to concentrate resources, and some of the capability we have talked about is very expensive. I was looking at one investigation this morning that has cost us £30,000 just in communications data. So there are breaks in the system as well, but the situation we are in is that we have to look at the highest threats—we are often looking at people who already have pretty long criminal records—and try to deploy the tactic against them. We just do not have the capability or resources to go into these sorts of fishing expeditions that were described.

The Chairman: Okay, I think we get the message.

Q1135 Lord Armstrong of Ilminster: I just wanted to come back to the question of what they call future-proofing. We have a Bill and Clause 1, which endeavours to future-proof by throwing its net very, very wide. That has alarmed people, as we have heard. Insofar as it is an attempt to future-proof, it is a very difficult thing to do in any other way because we do not know what the future is going to be, so the only way you can proof against the future is by these very general provisions. The alternative is something more limited now, to deal with today’s problems, and some kind of legislation in the future as new problems emerge. You will probably know as well as we do that there are great pressures on the legislative timetable. It is not easy to get legislation on such a subject frequently or quickly, and I wonder if you have any comments on that dilemma, because I think it is one of the dilemmas we face.

Sir Peter Fahy: I would totally agree with you. It seems to us, when you look at things like the potential development of 4G and other capabilities, that it is really impossible for legislation to keep up with that. Therefore, I would say that the alternative of the way you then operate the oversight regimes, the inspection regimes, the regulations that the Home Secretary may make
to control this form of activity, and the way that the courts then view that, is a much better safeguard than trying to go through the legislative timetable to catch up. That, for me, is the right way to try and get the balance, but, as Mr Davies said, we are not experts on this. I think the concern absolutely, in lots of areas we see, is just the way that technology and societal attitudes are changing, which is very, very rapidly. For legislation and some of our processes to keep up with that is becoming more and more of a challenge.

Q1136 Lord Jones: The Lord Chairman made his remarks about Clause 1 just now, really a summation of a predicament we face with the draft Bill. Should we presume that in the private councils of ACPO there have been debates—lengthy debates, concerned debates? Does ACPO really get its teeth into the issues before it presents itself publicly?

Sir Peter Fahy: Absolutely. We have had a lot of discussion about this particular issue and, as I say, some really serious concern and worry about, essentially, what we are going to do in the future, if we lose some of the capabilities that we have at the moment, because we have become so reliant on them. Things like interrogation, which perhaps worked 30 years ago, are no longer the tactics that we use.

Q1137 The Chairman: Let us be clear: you are not calling for them to be brought back.

Sir Peter Fahy: Indeed; I have been around a long time too. It is about having to get absolutely hard evidence from technology. But obviously there is a lot of angst at the moment about the level of public confidence and about questions of police integrity, and we treat that very, very seriously. And obviously there has been a lot of debate as well about, when issues become party-political—and there is an operational policing issue in there—how chief constables intervene to get the point across. We do treat that very seriously, because I think most of us think it is incredibly important that policing stays out of party politics.

The Chairman: I assure you I shall water-board Lord Jones later on.

Peter Davies: I would just like to offer a thought about Lord Armstrong’s question. I do not think the basic principles of what communications data should deliver change. They are about subscriber information, service use information, and traffic data. What changes is where you might look for those pieces of data in a changing technological world, where people are far more adept and use social networking, for example, or gaming technology as their chosen means of communication. Those are the things that change. The principle of what we are looking for is exactly the same. Although some police habits have changed, as we have noticed over the last 30 years, looking for that kind of data, whether it is on a landline telephone or in the technology of five years’ time, is what this is about. If it is possible to frame some legislation that enables law enforcement to carry on doing that, whatever the technological means by which that data may be found, that is what I think would be in the best interests of protecting the public.

Q1138 The Chairman: So we can put the principles into a Bill, which we amend every 10 years, like RIPA. If we were to be able to recommend to the Home Office, and if the Home Office were to be able to find machinery whereby the technical bits of where it can be found could be amended by order every year, by the Minister and through parliamentary scrutiny, you would be happier then that Clause 1 was not so wide-ranging.
Peter Davies: I would be happy enough. I keep repeating myself. I am not a legislator. I am not an expert on framing legislation, but I can tell you what the operational requirement is: it is as I have articulated. The best way of enabling people whose concerns are the protection of the public to access that communications data when they need it, in a proportionate, lawful, accountable and safe way, is what we are looking for. What you have just described does not sound like the worst of the options, by any means.

Q1139 Dr Huppert: Mr Ellis and I do not always agree on everything to do with this issue, but there is one thing I just wanted to agree on, which is that some of the media coverage in this area has not been very accurate. There is a risk about overstating what it will do, but also understating it. There was an article in the Sun at the beginning of this that said, “Only suspected terrorists, paedophiles or serious criminals will be investigated”. Presumably you would not want to see inaccurate statements like that made when it would be used far wider. Is that correct?

Sir Peter Fahy: Yes, absolutely.

Q1140 Dr Huppert: That was the Home Secretary’s article, so I hope we will hear from her tomorrow how she would correct it.

Sir Peter Fahy: There has obviously been some debate as well recently about the growing workload we are getting from investigating harassment on things like Facebook and some people seeing that as fairly low level. On the other hand, if a young person, God forbid, commits suicide because of bullying and harassment, the coroner may well have something fairly direct to say to the police force, such as, “Did you do everything to try and investigate that?” So I think that shows that these are serious issues, and that is why it has been difficult for policing overall and legislators to frame what is serious crime. Because often it is a bit like the guy texting on the motorway: it only becomes really serious when you see the consequence of whether somebody died as a result. That is part of the complication in this area, but as Peter and Mr Davies have shown, activities on the internet—that form of communication, the ability to commit crime on the internet, whether it is stealing goods and getting them delivered to bogus addresses or some of the other activity—is clearly an increasing part of our work.

The Chairman: Thank you very much. We have had a long but very worthwhile session. We are very grateful to all of you for coming here today. Thank you all very much. Your evidence has helped the Committee again slowly to claw its way towards a possible solution, or a possible report for the Home Office to come up with a solution. Thank you very much.
WEDNESDAY 31 OCTOBER 2012

Members present:

Lord Blencathra (Chairman)
Lord Armstrong of Ilminster
Baroness Cohen of Pimlico
Lord Faulks
Lord Jones
Lord Strasburger
Mr Nick Brown
Michael Ellis
Dr Julian Huppert
Stephen Mosley
Craig Whittaker
David Wright

Secretary of State for the Home Department [Rt Hon Theresa May MP] (QQ 1141-1207)

Examination of Witness

Witness: Rt Hon Theresa May MP, Secretary of State for the Home Department, examined.

Q1141 The Chairman: Welcome, Home Secretary, to our deliberations. You gave us a very tight deadline to review the Bill. We believe we have been assiduous in covering all aspects of it. We have held three evidence sessions per week, so that we could have as thorough an understanding as possible. We have collected thousands of pages of evidence, and we are now at the end of our evidence-gathering session. We are very grateful to have you with us today. That is all from me. Do you have any opening statement, Home Secretary?

Mrs May: Certainly I am aware that there has been a lot of discussion around Clause 1 and the interpretation of Clause 1.

Mrs May: No, Chairman, save to say that I am conscious of the tight deadline that we set you, and I am also very conscious of the diligent way in which the Committee has been proceeding with its scrutiny.

The Chairman: Thank you very much, Home Secretary.

Q1142 Michael Ellis: Home Secretary, good afternoon. We heard from senior police officers yesterday who, amongst other of our witnesses, have spoken powerfully about the operational need for a bill along these lines. One of the concerns that has been expressed to us by some witnesses, and by others, has been the breadth of the powers that are given to the Secretary of State by Clause 1 of this current draft. The Home Office officials that came before us recently said that this was an issue of drafting, rather than intent, and clearly we appreciate that this is a draft Bill. But they said they would be going back to Ministers about this. Do you accept that Clause 1 is wider, or can be interpreted to be wider, in its current drafting than it need be?

Mrs May: Certainly I am aware that there has been a lot of discussion around Clause 1 and the interpretation of Clause 1. From what I can see, people have been interpreting it in a way that
was not intended when it was drafted, and certainly we would be willing to look at the drafting, to make sure that that perhaps meets our needs and cannot be misinterpreted in the way that it has been. There is, however, an element to Clause 1 where I think that it is important that we have a degree of flexibility. It is about getting that balance right. However, it is important that, as things are ever-moving in the technological field, we are able to build into the Bill a degree of flexibility, subject to appropriate procedures and so forth in future. Obviously, the orders and so forth would go through Parliamentary processes, but that flexibility enables us not to have to constantly come back, if there is too tight a definition.

Q1143 Michael Ellis: Because of the speed and the advance of this area of technology.

Mrs May: That is right. We know what we know now. We can do a certain amount of prediction for the future, but, of course, even by the time the Bill would come in, on a normal timetable—were it to be introduced in this session or the next session—it would be a few years on before this came into play. By that time, things could have changed, and having the ability to have that flexibility as technology changes is important. Because the aim of this, as I think everybody knows, is to ensure that our law enforcement agencies can carry on having access to the data that they find so operationally necessary in terms of investigations and catching criminals and saving lives.

Q1144 Michael Ellis: Now, some of the CSPs have told us that what your officials have proposed in private discussion seems to them to be narrow, proportionate and reasonable. But they have a concern that the Bill will empower a Secretary of State to do a good deal more. Therefore, assurances about the way it is intended to use powers do not necessarily preclude the possibility of abuse in the future, so I wondered if you had any observations about the possibilities of abuse, and the protections that you feel are in place to prevent abuse, should there be any attempt to misuse powers in this area in the future.

Mrs May: The first comment I would make is that, obviously, we have had a number of discussions with a number of CSPs over time, leading up to this draft Bill. 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, so there is a limited scope for the data that we want to have access to. We have been very clear about that at every stage, and the Bill is not intended to take us any further than that.

Q1145 Lord Strasburger: Good afternoon, Home Secretary. I am very pleased to hear what you have to say about not wanting to capture content. What I say in my emails is my business, and not the state’s. Similarly, would you agree with me that records of which websites you or I or anyone in this room visits—for example, perhaps, Alcoholics Anonymous or sites about coping with mental illness—could reveal very private information about the person’s life, and, in reality, is content, and so should be outside the scope of the Bill?

Mrs May: I am grateful to you, Lord Strasburger, for giving me another opportunity to confirm that we do not want to look at the content of people’s emails. This, sadly, is one of the myths that has appeared in public, and I can reiterate that that is not what this Bill is about. On the issue in relation to the websites that somebody has visited, first of all, we are not in the business either of trying to get into information about personal details of individuals. As I say, communications data is about the who, when, where, and how.
However, if somebody has visited a particular website, that may actually be relevant to an investigation. If CEOP is investigating a ring of child abusers, the fact that an individual has accessed a website that shows photographs of child abuse may be relevant to that investigation.

Q1146 Lord Strasburger: We have heard that the use of DPI black boxes at service providers to monitor internet activity at a national scale is only currently being done in China, Iran and Kazakhstan. How do you feel about the prospect of becoming the first democracy to join them?

Mrs May: There has been quite a lot of discussion about the technicalities of how the access to the CD will be undertaken. I am sure you have had quite a lot of evidence about exactly what those technicalities will be. All I will say in response is that obviously we can go into more technical detail for you if you would like, but I do not perceive what is going to happen as a result of this Bill in quite the terms that you do, in the way in which you have asked the question. I am very happy to come back in writing or for another private session, where we can go into some more of the technicalities of exactly what is going to be done.

Q1147 Lord Strasburger: We have had some difficulty in extracting from your officials the comparative information in terms of what is being done elsewhere in the world. This information, that there is no democracy in the world currently using or contemplating such draconian measures, is what we have heard from other witnesses.

Mrs May: Lord Blencathra, I am very happy to write to the Committee with some further detail, if the Committee is happy.

The Chairman: As urgently as possible.

Q1148 Lord Strasburger: During the public evidence session last week, your officials confirmed that, as was stated in your written evidence, the data gaps that you are currently seeking to fill are subscriber data relating to IP addresses and weblogs. Is there any reason why these, and access to third party data, should not be stated in the Bill as being the only new matters for which access is permissible?

Mrs May: It relates to an earlier answer I gave Mr Ellis, which is about the need for flexibility as we see technology developing. There are other issues about putting gap requirements on the face of the Bill, as well, in terms of some of the messages it sends, but if we were to put those specific requirements on the face of the Bill today, that might solve today’s problem but in a few years’ time we might need the flexibility to be able to deal with some other aspect of data. The reason for bringing the Bill forward is that we are seeing a degradation in our ability to access important data, which is needed operationally to catch criminals.

Q1149 The Chairman: Home Secretary, what if those elements were in an order-making power in the Bill, which could be amended very rapidly and brought before Parliament? I appreciate that if it is in the main Act of Parliament, one sometimes waits a few years to get a RIPA-type Bill. Would you be happier with that, then?

Mrs May: I think, as I say, there may be some other arguments for not always specifying where you think your gap is, in terms of the message it sends to everybody as to what they can
suddenly start using. Certainly, there would be a difference between having it in primary legislation and having it in some secondary legislation with Parliament able to look at it.

**Q1150 The Chairman:** It could solve the problem of future-proofing. Having an order-making power that could rapidly plug some of these technological changes could deal with the future-proofing problem. I think we accept your point that you might not want to see it for other reasons.

**Mrs May:** Certainly, that would be a way of enabling Parliament to have a look at any future-proofing requirements. I come back to the point that there is an advantage and a benefit to us from being able to retain a sufficient degree of flexibility in the Bill itself that we do not find ourselves hamstrung in the future, in the way that we are at the moment.

**Q1151 Lord Jones:** We understand that one reason the powers have been so broadly drafted is to attempt to deal with future developments in communication, without having to go back to Parliament. That is how we have seen it. The Committee wonders whether it would not be better to devise a procedure for Parliamentary approval that is more rigorous than affirmative resolution, but less time-consuming than primary legislation. Would you entertain that?

**Mrs May:** I can well see that the Committee might wish to look at an issue like that. I am not quite sure what that procedure could or might be. I come back to my point that I said right at the beginning, that it is important to maintain sufficient flexibility to allow change to take place to meet growing technological needs. Otherwise, we see criminals slipping through the net.

**Lord Jones:** There are two former Chief Whips here who could be of service on parliamentary procedures.

**Mrs May:** Former Chief Whips can be of service in many ways, Lord Jones.

**Q1152 Lord Jones:** That was how I found it, when I was in the other place. My second question is: would a possible procedure be one of consideration by a Parliamentary committee with the power to call for evidence, and to make recommendations, to which the Government should reply?

**Mrs May:** If you were going to go down that route of some parliamentary procedure, there are a number of ways in which that could be done. I come back to my central point, which is that what we want to be able to do at any point in time is to ensure that our law enforcement agencies have the powers necessary to do the job we want them to do, of catching criminals and saving lives. We would be concerned about any procedure that takes a significant amount of time and that means that we see criminals slipping through the net.

**Q1153 Lord Armstrong of Ilminster:** Secretary of State, I quite see the need for flexibility in Clause 1 that you have been speaking about. But, of course, the more flexible it is, the greater the concern that it gives rise to about possible intrusions on privacy. There is a balance there to be struck, which is for Parliament and for you to strike. I wonder if you would like to comment on that aspect of it, and whether it would be acceptable to have a narrower degree of flexibility if there could be some procedure whereby you could move very quickly to extend the powers.
Mrs May: In a sense, Lord Armstrong, you have hit the nail on the head, if I may say so. This is, as you say, a balance between protection of privacy and the issue of government being able to ensure the law enforcement agencies have the powers that they need. As I say, my concern is to ensure that there is sufficient flexibility and that we do not just find ourselves introducing a Bill that has gaps in it as soon as it comes into play, and has only achieved a limited extension of the ability of the law enforcement agencies to do their job. From the nature of the questions, obviously the Committee will be looking at other procedures that could take place to reduce that flexibility. We would obviously look at any ideas that the Committee brings forward, but, as you say, the crucial issue is where that balance lies.

The Chairman: That is very helpful, Home Secretary.

Q1154 David Wright: Home Secretary, I welcome your opening remarks about the scope of what the Home Office wants to secure in terms of this legislation. Perhaps coming at it from a slightly different angle, my concern would be that as technology does change and content becomes more and more difficult to draw out—the more it merges in terms of content and subscriber data—aren’t you concerned that you will end up in a position where you will find yourself hamstrung, because of the wide scope of the Bill and your direction to want to ensure that content is not included? So that is the other side of the argument, that it could go either way here. Giving a future Home Secretary, or yourself, the capacity to come back to Parliament to confirm the types of communications data that you want may actually be quite useful.

Mrs May: You are tempting me down a road, Mr Wright.

David Wright: I am trying to.

Mrs May: Obviously, one of the issues that is already in play is this question of how, given that we only want certain information, you separate that from content. We spent quite a long time looking at the technology on this, and I think it has been clear from some of the technical experts that have given evidence to the Committee that it is possible to separate content out from the who, when, where and how. Therefore, I am reasonably confident in terms of that. Now, you are talking about maybe some years down the line.

Q1155 David Wright: Five years down the line, we could get a piece of kit that changes the whole parameter of the game. That is the problem, isn’t it?

Mrs May: If, at some stage in the future, it became the case that you could never separate content from the communications data as we describe it, then that would be a different discussion that would need to be had.

Q1156 Baroness Cohen of Pimlico: We all feel that the British public would like policemen, security services and proper authorities to be able to access the data they want, and yet, on the whole, we do not really believe in the concept of future-proofing. We think that there is where the difficulty lies. In trying to do that, you are alarming—probably unnecessarily—the civil rights people. All of us are interested in civil rights. That wide flexibility, if misused, really will cause trouble. I am really commenting that this is going to be an urgent one to solve. While we are, I think, on the same side, this one is going to be difficult to solve.

Mrs May: I accept the point. Certainly, one of the issues that has come through quite clearly is this question of drafting, and whether the way in which the clause has been set out has given
rise to concerns that need not be there, in terms of the intention of the Government. That is why, certainly, this is one of the issues that we are willing to look at, to make sure that we have got the best drafting to relay our intention and not raise those sorts of concerns for people.

**The Chairman:** I am fairly certain, Home Secretary, that this is an area on which the Committee will be commenting.

**Q1157 Stephen Mosley:** We have received written evidence from the intelligence and security services, saying that they believe they need the full range of powers detailed in this Bill. Now, the Lord Chairman has asked yourself if we could have permission to interview formally those services, either in public and private, and you have turned us down. If they were here, I would want to ask them if they could explain to us why any lesser powers would be inadequate.

**Mrs May:** To address the point that is made about the appearance, or not as the case is, of the security and intelligence agencies, one of the reasons why I asked the Intelligence and Security Committee to do a separate and parallel piece of work and liaise with this joint scrutiny committee is because I recognised that there would have been certain issues that not only could not have been revealed in private session to this Committee, but can only be revealed to the Intelligence and Security Committee, whose job it is to oversee the security and intelligence agencies.

My answer to why it is necessary to have these powers, and why it would not be possible to have lesser powers, is that if we look at what we are trying to do, what we are saying is that, at the moment, the law enforcement and security agencies have access to certain data that enables them to pursue investigations. I think the figure is that 95% of serious crime investigations over the past 10 years have involved some form of communications data, as has every major terrorist investigation. This is data that is currently necessary and used by the agencies. What we want to do, obviously, is to make sure that as the technology develops and people communicate in different ways, they are able to have access to the same type of information on these different forms of communication. So the answer to your question would be that, if they were only able to have something less than that, that would effectively be the equivalent of a degradation of their abilities.

**Q1158 Dr Huppert:** It is good to see you here, Home Secretary. Can I just firstly clear something up? In the *Sun* on 3 April, you wrote, “Only suspected terrorists, paedophiles or serious criminals will be investigated” using this Bill. Clause 9 is currently written very much broader than that. Do you think, therefore, we should be recommending that Clause 9 be redrafted to tighten it to your stated intention?

**Mrs May:** We have certainly got no intention of setting out any permitted purposes beyond those that are in the draft Bill. There is one addition to the purposes that have gone in that is different from those that exist at the moment, in that we are putting in a reference to the Financial Services Authority that replaces something that is being repealed in the Financial Services and Markets Act 2000 in relation to market exposure. Again, it is back to this issue that the more you prescribe on the face of the Bill, the more it tightens your hands, and the more difficult it makes it if the scope, in due course, does need to be extended.
Q1159 Dr Huppert: Can we just be clear on your intention? Is it your intention that this Bill would only be used, as you wrote in the *Sun*, for suspected terrorists, paedophiles, or serious criminals?

*Mrs May:* That is the current scope of the way in which the use is made. There are obviously some other public authorities at the moment who have access to communications data, beyond those that are on the face of this Bill. As you will know, we have been doing an exercise to look at those bodies, to see whether it is right that they be given the powers that are in the Bill. I think it is true to say that you might find it difficult to describe some of the individuals with which those bodies are concerned in those three categories. But the main purpose of the Bill is, certainly, to cover the categories of people that I set out in that article.

Q1160 Dr Huppert: I will move on to the obligations that this would impose on telecommunications providers. We have heard from a whole range of them, both domestic and overseas, that it would potentially involve restructuring their systems and a very large expenditure, for which they would be reimbursed from the public purse. There has also been an issue that they say—to summarise a whole lot of different responses—that there have not been that many clear consultations. I know your officials say there have been, and there is a discrepancy there, but Charles Farr, when he appeared last week, accepted that there should be much further consultation on the detail of the Bill. If this Bill does proceed any further, how will you engage and consult with them so that—if the Bill does make any progress—they would say that there has been consultation and they understand what is proposed?

*Mrs May:* We have had good discussions with a number of CSPs in the run-up to this Bill being drafted and published. We would certainly aim to continue that. Obviously, going forward, we would expect the discussions that would be held with the various providers to become more technical and more detailed, because there would be issues about how the system would actually work, and making sure that assumptions and discussions so far stood further testing to make sure that we got it absolutely right. It is the case that we have been having discussions with both UK CSPs and overseas CSPs, and we will continue to do so.

Q1161 The Chairman: Can I interrupt? Were those discussions specifically about the draft Bill, or were they just discussions in the past about communications data in general?

*Mrs May:* They have been of both types, Lord Blencathra. They started off being more general, but have then become more specific about the Bill: about the requirements, about how those requirements could be met, and about what any powers in a Bill should be.

Q1162 The Chairman: Most of the telecoms operators tell us that the first discussions they had on the specific provisions in this draft Bill were after publication, and some of the CSPs say that the first consultation they had was the day after we summoned them to give evidence.

*Mrs May:* We are into a definitional issue here, in the sense that it is only possible to consult on aspects that are in a draft Bill when the draft Bill has been published. It is possible to discuss the issues that then become clauses in a draft Bill afterwards.

The Chairman: Thank you, Home Secretary. I think you have been very careful in your choice of language. I congratulate you on that.
Q1163 Dr Huppert: If I can move on to another group—we have not been able to talk to anything like all of these—we have had a lot of representations from members of the general public about this issue. Those who have contacted this Committee—and there have been very many thousands, I believe—have been almost uniformly hostile to the Bill and very, very critical of the breadth of the powers as set out in the legislation, which may be different from what the Home Office intends. You may also be aware that there was a YouGov poll done for Big Brother Watch, which found that 6% of people thought that the Government had made a clear and compelling case for the Bill. There is a lot of very genuine concern about this Bill, and the effect of intrusion into private lives, given the breadth of it. What steps will you take to try to reassure people that that is not something that they should be concerned about?

Mrs May: I am aware that there has been a lot of concern, based partly on the publicity around the Bill that portrayed a number of myths about the Bill, such as that it was going to enable the Government to read everybody’s emails, which it plainly is not. The other aspect that we have not got across to people that it is not the case that the Government is going to be seeing the who, when, where and how of every single person’s communications. Data will be retained by the CSPs, but it will only be possible for law enforcement agencies to have access to it when they have an investigative reason for doing so, and they have to make a clear case. It goes through the process. I believe that the Committee has visited the Met, and seen the single point of contact operation and the process that is gone through to make sure that that data is only requested in cases where it is indeed necessary in an investigation.

Of course, it is not just the case that data has played such a significant role in so many serious and organised crime cases and terrorist investigations, but I think it was between April and June of this year that, it was something like—I may need to check these figures—46 out of 53 prosecutions from the CPS used this data as part of those prosecutions. So it is not just the police accessing it in investigation: it goes through into prosecutions. And if I may, Dr Huppert, I believe that I did not say in The Sun article—I do not have it in front of me—that it would “only” be used in relation to serious crime and terrorism.

Q1164 Dr Huppert: The exact quote is, “No one is going to be looking through ordinary people’s emails or Facebook posts. Only suspected terrorists, paedophiles or serious criminals will be investigated.” That is, for what it is worth, the quote, but that was back in April. If I could just ask one final question, Lord Chairman: there has been a lot of misinformation and lack of clarity around this; I think we would all agree with that. Given that, are you grateful we have had the chance to go through this pre-legislative process, where yourself, police, and other people have had the chance to state publicly what they think about this, and that it has highlighted a number of things that—as officials have already accepted—would need to be updated in the Bill?

Mrs May: I certainly think this has been a good process. As I say, I am conscious of the length of time you have given to do this. It has shown an open and public discussion about this in a way that has been very important. Obviously, I think some of the evidence that you have received, particularly from the police, has highlighted the operational necessity of this, and I think that has perhaps hopefully sent a message that we previously had not been able to get across to people.

---

4 Mrs May subsequently made clear that the article to which she was referring was a later article in The Sun on the 14 June 2012
Q1165 Lord Strasburger: If this Bill were enacted, there would be a massive increase in the data being held about every citizen who uses the Internet. This data would be a honey pot for casual hackers, blackmailers, criminals large and small, all over the world, and foreign states. Given the woeful record of public and private sector organisations in protecting the data they hold from loss or theft, why should the public have any confidence that their private and financially valuable data will remain secure?

Mrs May: Security of data is always a concern for people in their everyday life, in the way in which they use data today, let alone this. It is not the case that suddenly people should start worrying and they do not need to worry today. One of my personal concerns is that a lot of people today probably do not handle their data in as secure a way as they could be handling it. But this is not about the public sector. You said the public sector was woeful.

Lord Strasburger: And the private sector.

Mrs May: Let’s get the public sector out of the way, because this is not data that is going to be held by the public sector. This is data that will be held by the private sector, by the CSPs. Obviously, we have been talking to them about the security of that data. There will be, as you know, some duties in the Bill in terms of any breaches in relation to the security of that data. We will be doing everything we can to ensure that that data is held securely, as the data is held today. CSPs are holding significant amounts of data about people’s communications as we speak. This is not a new concept.

Q1166 Lord Strasburger: The Bill would require the CSPs to hold a lot more data, a wider range of data, and 12 months’ data. What will be new is that there will be a lot more data about a lot more things being held.

Mrs May: They will be holding more data. They will be retaining it for 12 months. That is what they do on some of the data today, anyway. So the concept of the private sector holding data, and whether or not that is secured for individuals, is not changed by the nature of this Bill.

Q1167 Lord Strasburger: We have heard from experts, including some of the CSPs, that they have actually had concerns about their ability to withstand attacks, given the increased amount of data and the increased attractiveness of this data. I have got a list here of some of the breaches that we know about in private sector organisations: NASA; Microsoft; Yahoo; Bank of America; Citigroup; Apple. LinkedIn had 6.5 million passwords stolen a few months ago. They are all vulnerable, and owing to the fact that this data is being expanded and is going to hold, arguably, some very private information, many people are concerned that this data will get out there. In fact, some of the experts have told us this data will get out.

Mrs May: First of all, if I come back to the central point of why we are doing this—which is the who, when, where and how—that is the data that we will be requiring to be held. That is what we want to be able to have access to. That sort of data is held already. I am aware of the issue that you raise about issues with systems today. I do not think the fact that there is going to be a different set of data, in the sense of different communication forms for the same type of data, and that is going to be held, changes that principle. Government has to take a decision. We have to decide whether we want our law enforcement agencies to be able to
carry on doing what they have been doing, which is bringing people to justice and saving lives, or not.

**Q1168 Stephen Mosley:** The weakest point of any computer system is the human. You talked about sanctions, but as I understand it, most of them are sanctions on the CSPs to make sure that they protect their data. What about the situation where people in authority, whether it is the police or other organisations, misuse access to that data? Do you think there should be criminal sanctions in that situation?

**Mrs May:** There are already procedures in place. If somebody in the police misuses access to some form of data, then it is already possible to take some action against those officers. For example, if an officer misuses access to the police national computer, and that is identified, then action can be taken against that officer. So there would already be procedures in place that would enable some form of action to be taken. Obviously it is already the case, also, that this is not just about misconduct. In some circumstances, if it can be seen that there is an element of criminality in terms of misconduct in public office, or something like that, then action can be taken on those lines.

**Q1169 The Chairman:** Home Secretary, I do not think we have seen any examples of police breaking the rules, but do you think it would show even-handedness to the public, and help reassure them, if there were criminal sanctions for the CSPs or the internet service providers who break the rules, and there were equally serious criminal sanctions for the police officers? Even though we have no evidence that police have actually done it?

**Mrs May:** Certainly I have seen no evidence that the police have mishandled or misused any of this information that they have had access to up until now. What I am trying to say is that there are already sanctions—that may be of a slightly different kind from the sanctions that appear on the face of the Bill—already available in relation to the police, should they misuse data.

**Q1170 Craig Whittaker:** Home Secretary, good afternoon. We have heard a lot about the spirit of the Bill, and we heard evidence that large CSPs will probably be the only ones asked to collect this information. The face of the Bill does not say that at all, so you can understand why some people are sceptical. I want to ask you about SMEs who do not have the personnel to perform some of the tasks that would need to be done to collect data. What risk assessment has been done around SMEs, and what damage will that do to business set-ups and, indeed, innovation in the UK in this field?

**Mrs May:** We have looked at that issue. On the innovation point, I think I am right in saying that the Minister for Science and Innovation, David Willetts, set out clearly in the Business Department’s evidence that they did not see that this would in any way harm innovation in the UK. In relation to SMEs, you are absolutely right. As has been made clear, there would be certain CSPs that the Government would be naturally dealing with. There would be some very small CSPs and start-ups where they would not necessarily be doing so. If it were felt, because of any evidence, that we should be doing that, then of course appropriate discussions would be held with those bodies about their capabilities and how this could be managed. But it is not the intention, as you have said, to suddenly have an interaction with every single CSP,
because we are conscious that there will be some smaller providers who do not have the capability to be able to do what is being requested.

**Q1171 Lord Strasburger:** When agreeing the policy of the draft Bill, you were, of course, aware of the views of the intelligence, security and law enforcement agencies that their work requires additional access to communications data. Did you, before deciding on the breadth of the new powers, consult any of the organisations concerned with protecting privacy and human rights?

**Mrs May:** There have been, throughout the course of this, a number of discussions with certain organisations about their views on this.

**Q1172 Lord Strasburger:** Could you elaborate on that a bit?

**Mrs May:** For example, I have had a very early discussion on this and a number of other matters with, certainly, one organisation. Officials have been discussing, have had other people in, and have had a number of meetings with individuals and organisations who take a different view from the Government.

**Q1173 Lord Strasburger:** But you personally have not had very many, by the sounds of it.

**Mrs May:** No, because that would naturally be conducted normally by officials. Obviously, they would feed back the information to me.

**Q1174 Mr Brown:** We touched on the offence of misconduct in public office in your earlier reply to us. The general public, our constituents, are frightened that they are going to be spied on and that people will obtain information about them, perhaps unlawfully, and that somehow it will then come into the public domain. Now, one way of reassuring the general public would be to ensure that those who break the law are caught and punished. The Information Commissioner said to us, repeating a call that he has made before, that if we enacted Sections 77 and 78 of the Criminal Justice and Immigration Act 2008, that would meet the case. In other words, the offences are already set out in legislation, but they have not been enacted. What would your view be on bringing in a modern and proportionate offence that could be prosecuted?

**Mrs May:** I think in relation to the particular offences in the 2008 Act, if I may, Mr Brown, I would like to go away and have a look at the specifics in that, and perhaps write to the Committee on that point. I appreciate the point that the Committee is making that the public want to know that if somebody does bad things or things they should not be doing with their information, that there is going to be some appropriate sanction on that individual. How that is undertaken, whether it is new powers or not, is a question that would need to be looked at. I am happy to look at the specific offences that are in that 2008 Act.

**Q1175 Lord Faulks:** Home Secretary, I think that particular point was one that was raised before the Leveson inquiry, and I think it is likely that he may have some observations to make when he produces a report fairly shortly.

**Mrs May:** Thank you.
Q1176 Lord Armstrong of Ilminster: If I may revert for a moment to the permitted purposes in Clause 9 of the Bill. As I understand it, Clause 9 repeats the 10 purposes that are derived from RIPA, and then Clause 9(7) would allow you to add further purposes. The House of Lords Delegated Powers and Regulatory Reform Committee have said that they would not necessarily find that extra power acceptable, just because it derives from the existing power in RIPA, which they at the time thought too wide. If somebody said they wanted to extend the permitted purposes, what justification would you be expected to require? 

Mrs May: The first answer would be that this would need to be a purpose that I felt was necessary and proportionate in its operation. I think the last time a change was made to existing powers was in 2006, and that was to added purposes relating to investigations into miscarriage of justice and the obtaining of information about persons who have died who are unable to identify themselves, which were consolidated in an order in 2010. What I hope is that that shows the sort of nature of purpose that might be used as an extension in relation to this, but it would have to be necessary and proportionate. It would have to be something where there was clearly a public benefit for adding that purpose, which outweighed the concerns that there might be about that information being accessed for that purpose.

Q1177 Lord Armstrong of Ilminster: May I turn from that to the public authorities? The Bill defines the four relevant public authorities with access to communications data. Clause 21 would give you power to add to that list, and your memorandum says that, “circumstances may change over time such that an existing body may be able to present a compelling case for designation”. It rather looks as though you do not really believe that any other body than the four relevant public authorities—the police, and so on—really need to be designated, but we have seen cases made to you for extension. I would be glad to know whether you think you are going to need to designate a number of other public bodies beyond the four.

Mrs May: It has been a very good exercise for us to not assume that the existing list of public authorities should naturally translate into the new Bill, but to ask those public authorities beyond those that clearly are currently the majority users of the communications data to justify its access. Now, in some cases, they do not have very many requests that they make. In others, it looks quite small compared to, say, the police, but actually it is a reasonable number in relation to the agencies. Currently, my view is that there are those for which it is possible to make a case. I would cite, for example, the UK Border Agency, and I have already mentioned the Financial Services Authority. Further than that, there are others that we are still looking at, and there will be some where, actually, a good case has not been made.

Q1178 Lord Armstrong of Ilminster: Would you be prepared to consider whether any other additional bodies that were designated should, when applying for access to data, need to go through a procedure more rigorous than that required of the police, intelligence services, SOCA and HMRC? I am thinking of, for instance, something like the National Anti-Fraud Network, which I believe is a central institution that can handle local authority applications, and has the expertise—the SPOCs, and all that—required to do so. Would it be in your thoughts that if there were other bodies than the serious crime, intelligence and security agencies designated, that they might be put through a more rigorous procedure through some kind of central body like that?
Mrs May: I have a natural disinclination to creating new central bodies, but I think what we would need to do would be to look at each individual case and the extent to which they were able to show that they had, or were able to provide, sufficiently robust procedures, before then looking to whether there were a number of organisations where it was perhaps felt that a central body would be more appropriate. The difficulty is, obviously, for those bodies who do not use this very often, ensuring that they have a truly robust process, i.e. that somebody actually understands the full process, because the police are used to doing it. They have an operation that is streamlined and smooth. For some of the organisations that request access very regularly, there is a question, first of all, as to whether it is right for them to continue to have access, and then if they do, how it is appropriate to make sure that the public can have confidence that they are not doing this capriciously and that they are doing it properly.

Q1179 Lord Armstrong of Ilminster: That sounds as if your mind is not closed to the idea of some kind of central point for these other authorities. At the moment, each separate police service has its own systems of authorisation for access to communications data. There is some suggestion that there might be a case for centralising some of that, and that some of the smaller police authorities might conceivably go to a central police pool of SPOCs, and so on. The central body would have the expertise and the experience to handle it, and it would save the smaller authorities having to develop their own authorisation procedures.

Mrs May: On the first remark, if I may, Lord Armstrong, I think it would be ill-mannered of me to come before a joint scrutiny committee and say that I was closed to absolutely any proposals that the joint scrutiny committee might choose to bring up in its report. I had not considered fully the question of police forces going to a central point. My view would be that police forces are able to provide the robust processes internally. They are more used to dealing with this sort of request, and I think they have naturally the proper structures and hierarchies and processes in place that enable them to make these sorts of requests properly, without having to go to a central authority.

Q1180 The Chairman: I think, Home Secretary, we have heard that Devon and Cornwall, Wiltshire, and possibly another force have decided to centralise their SPOC system for reasons of efficiency, higher-quality training, and so on. So if that were to be the case, you would not be adverse to other police forces—without amalgamating police forces—at least sharing their SPOC resource?

Mrs May: There are many good examples of police forces who are now sharing resources across a variety of different areas. If they choose to do so, because it makes sense for them and is efficient, then I am very happy for them to do so. What I am less willing to go down the route of is to say that the Government will mandate that they will all go through a certain structure. If they are going to share services, they need to do it with the forces that make sense to them, where they have got some natural affinities, where it is going to work, and where perhaps they are sharing other resources as well.

Sitting suspended for a Division in the House.
On resuming—
Q1181 David Wright: Home Secretary, could I just place on the record this issue about designated bodies on the face of the Bill? The idea of getting them to review whether they need to be able to access communications data is excellent, but I understand that a number of them have not replied to the consultation, which perhaps demonstrates that they do not need communications data or perhaps they are not very good at communicating. In terms of what is on the face of the Bill, if it is going to take some time for the Government to put this Bill together after this pre-legislative process, do you think it is going to be reasonable to specify on the face of the Bill the bodies that you want to have access to communications data?

Mrs May: Obviously, we need to specify certain bodies—those bodies that are going to have most access to it. I have a hesitation for trying to specify every single body that should have access on the face of the Bill, for a couple of reasons. First of all, it may be that by the time we have been through all of this process we will have had answers from everybody and we will have been able to make those judgements, but on a sheer practical point, bodies change. They change their names; they change their purposes; there are amalgamations, and so forth. I think if you are too prescriptive, you just end up with a situation where the legislation has hampered you and hamstrung you in a way that it was never intended to. So there is a practical issue there, and there is a value to the process of saying that there should be a consideration of any body that can be added to the list of those that have these powers and going through that process, rather than just having an approach of, “We will put everybody on the face of the Bill”.

Q1182 The Chairman: Home Secretary, on that point, would you accept that even if you whittle down the public bodies from 600 to 400, and then to 300, it still could cause public concern? On the one hand, there may be this misconception that, “The Government can tap into all my data and is going to collect massive amounts”. On the other, it is not just the security services, the police and the FSA; there are 400, 500, or 600 other bodies who could access it. Therefore, I think you seem to be edging closer to having on the face of the Bill the current big four, maybe the FSA or UKBA, a few of the big, important national bodies dealing with crime, national security, terrorism, children and so on, and then make all the rest go through extra, additional hoops, much stricter than you have at the moment, to make them justify access to even more limited data. Would it be fair to say you would be mindful to think of that?

Mrs May: What I am mindful of is a process where there is a second stage for those bodies, which is a consideration by Parliament as to whether they should be put onto the list of authorities that can have access. Then, there is an extra scrutiny for those bodies as to whether it is appropriate. I think one of the justifiable concerns has been the long list of bodies that currently exists, and people question why some of these organisations should have access to this sort of data. Now, for some of them, obviously we would not be talking about them having access to certain types of data. It might be more restricted. But I think there is a necessity that there is a separate process for these bodies, an extra rung on the ladder that they have to get up, in order to show that people can have confidence that these are bodies that are appropriate to have access.

Q1183 Stephen Mosley: Before the break, you said you had an aversion to creating new central bodies. However, the Bill does allow you to create a new central body to manage the
filter. Have you given any consideration, since the publication of the draft Bill to where that filter would reside? Would it be in the Home Office, an independent body, or somewhere else?

Mrs May: This is a matter that we are still giving some consideration to. There are obviously a number of arguments on either side of this. The filter is an important function to have. It does enable, in that completely unseen way, the information to be whittled down to what it is absolutely necessary for the law enforcement agencies to have, and that is a benefit in terms of the process. Where that resides and who oversees it is something that we are still working on. Obviously, as we develop those ideas, we will be happy to share them, but we are still looking at the pros and cons. As I am sure that every member of this Committee can see, there are advantages and disadvantages on all of these.

Q1184 Lord Faulks: Home Secretary, if I may, I would like to ask you about the ECHR and its application to this Bill. A very long and helpful memorandum was provided and attached to the Bill. It is obvious that, whatever else one may think about the scope of article 8—and this can be controversial—it is plainly engaged by the provisions of this Bill, involving as it does a potential invasion of people’s private lives. One of the justifications for it given in the memorandum is that the Information Commissioner and the Interception of Communications Commissioner will have new powers of oversight as regards the exercise and performance of the powers and duties conferred and proposed by the Bill. In fact, if one looks at the Bill—and I particularly have in mind Clause 22(5)—the Information Commissioner is told he must keep under review the operations of sections, including security, which, of course, is absolutely crucial to communications, as we have already discussed. He does not appear to be given those powers, or, on the face of it, any resources. And this is not just a technical human rights point, because he in fact gave evidence to us that he was concerned about the range of keeping under review aspects of the Bill, without having a clearly defined power given to him by the Bill, or in fact, the resources. Do you have any comment about that?

Mrs May: First of all, we believe that the Information Commissioner does have the powers that he needs to carry out the role that will be set out for him. There has been a question raised around resources, and we are in discussion with the Information Commissioner about that particular issue. I am always hesitant when a questioner starts with reference to the ECHR. I am never quite sure where we are going to go down. As you know, we have had long debates about the qualified nature of Article 8, and therefore its application in a whole variety of ways. We feel that the Information Commissioner does have the powers necessary to carry out his role and the various responsibilities that he will have, and, as I say, we are looking at the issue of additional resources. He said that he would need extra resources, but we are in discussion with him about that.

Q1185 Lord Faulks: The public clearly need quite a lot of reassurance about this, partly as a result of the misinformation on one side or another about what the scope of this Bill may be. The role of the Information Commissioner—indeed, the Interception of Communication Commissioner—is not, perhaps, quite as well known as it might be, compared with, let us say, the Independent Reviewer of Terrorism legislation. Does the Home Office envisage in some way raising the profile of that person or persons, so as to give the public rather more
reassurance that the potential exercise of these powers is reviewed by an independent person, and so that they can feel the weight of that independence?

_Mrs May:_ It is always difficult to find ways of getting across the role of somebody like the Interception Commissioner. I would say the Information Commissioner has probably more public prominence, because people do see cases, sometimes, where he has intervened or where the Information Commissioner’s office is commenting on various issues. I think it is the other commissioner that has less public profile. It is one of the problems across the suite of the commissioners, if you like, that they produce annual reports that are very well worth reading, but which most members of the public—indeed, I may say most members of both Houses of this Parliament—probably rarely read. However, I am afraid we do not have a “Let’s advertise the Interception Commissioner” campaign on the stocks, and I am not sure it would have much impact if we did.

Q1186 _Mr Brown:_ It is a framework Bill that we have under consideration, and I wonder if you have given any thought to how, if it were carried, Parliament might monitor the workings of the Act?

_Mrs May:_ I have every expectation that the existing structures of Parliament will have an interest in monitoring the workings of this Act. I am tempted to say that most Acts that are passed with a Home Office lead do come under significant scrutiny from the Home Affairs Select Committee quite regularly, but there are obviously other committees that do look at various aspects of issues like this as well.

Q1187 _Mr Brown:_ Do you think it would be an extra reassurance to the public if there were some further Parliamentary arrangement for post-legislative scrutiny, hearing reports as to how the powers under the Act are used, and providing a forum where people could complain if they felt that something had been done improperly?

_Mrs May:_ There is already a complaints procedure that people can take forward, if they feel that their data has been misused, so there is already a complaints path for people to use. I am not sure that adding a Parliamentary complaints path would necessarily add anything extra to the system.

Q1188 _Mr Brown:_ In a fast-moving world, do you not think there is a case for keeping the legislation itself under review, and considering whether it needs updating or reshaping as events and technologies move on?

_Mrs May:_ Part of the purpose of having some flexibility in the Bill is to make sure that we do not need constantly to be adapting the Bill and reviewing it as technology moves on. It is always open to Parliament to decide to do a piece of work on post-legislative scrutiny. There is more and more post-legislative scrutiny now being done of Acts. That is entirely in the hands of Parliament.

Q1189 _Mr Brown:_ But you are not opposed to it in principle.

_Mrs May:_ If I can put it like this, when I sat on the Modernisation Committee of Parliament, I was in favour of increasing post-legislative scrutiny.
Q1190 The Chairman: As I understand it, Home Secretary, you have got a technical advisory committee, which is a permanent committee advising on the technical aspects. Do you see scope for that being beefed up in some way, and maybe becoming part of some standing review committee under some Parliamentary authority, or with Parliamentary input, even?

Mrs May: I have no objection to looking at the technical advisory committee and saying, “Is it still, in the new circumstances, the right shape of body to undertake the job that we want it to undertake?” What I hesitate to do is to overlay everything with so many different committees and meetings and bodies that, actually, you end up with no real scrutiny at all, because everybody is falling over themselves to try to be the one body that is scrutinising the action of the Bill.

Q1191 Mr Brown: What would your attitude be to inserting a sunset clause into the Bill, so that it expired after a fixed period of time unless Parliament renewed it?

Mrs May: Because of the fast-moving world that you yourself described, Mr Brown, it is quite difficult to insert a sunset clause. I accept that that does not kick in unless Parliament decides; there is a Parliamentary procedure that looks at it. However, by their very nature, police operations are ongoing day on day. It seems to me that anything that acts to interrupt the ability of the police to have access to the data that they need to be able to catch criminals and save lives is a problem. The whole purpose of this is to say that we want a Bill that is going to enable our law enforcement agencies to have access to the information they need to do their job, and trying to overlay that with lots of scrutiny and boards and interruptions, and so forth, can just get in the way of what is—I believe—a very appropriate purpose, which is that we want our police and law enforcement agencies and others to be able to do the job of protecting the public.

Q1192 Baroness Cohen of Pimlico: The other answer to all of this is to improve the independent supervision. One of the exciting things the Information Commissioner produced was an overlay of the various surveillance commissioners, which was absolutely dazzling. I had no idea, as you suggest, and I also suspect that no member of the general public would know where to start. Would it be appropriate to suggest that the Home Office could consider de-complicating this structure, and does it lie with you to do so?

Mrs May: We did look at de-complicating the structure. In the consultation paper we put out on the Justice and Security Bill last year, we suggested an amalgamation of commissioners, to have a sort of super-commissioner—“Inspectorate General”, I think, or some such title. However, it was rejected. It did not meet with any high degree of support, publicly or elsewhere, and so we chose not to go ahead with it.

Q1193 Mr Brown: How have you satisfied yourself that the costs associated with the measures represent value for money? Specifically, can you say how you have accounted for inflation in the overall budget?

Mrs May: I am confident in the work that has been done so far on costs, but we are refining that. We recognise that we cannot just stand still on this. We are going back to talk to providers and others about the costs, to make sure that when we come to a Bill, we are able to give as good an approach as possible.
Q1194 Mr Brown: And inflation?
Mrs May: I believe inflation has been taken into account, but we are making sure that we take every single aspect that we need to take into account into account in the refinement. I am sure that has been done in the first place, but we are going back and having another look at it.

Q1195 Mr Brown: Parliament will have something in front of it.
Mrs May: There will be a proper impact assessment, which will set all of this out, yes.

Q1196 The Chairman: On costs, Home Secretary, nearly all of the internet service providers who talked to us were sceptical about the £1.8 billion cost. They all expect that to escalate, and not only because no government has ever brought any computer technology project in on budget. Looking at the other side of the coin, the estimated savings were up to £6 billion, and about £3 billion of that could have been on lives saved. Now, when we spoke to your officials, they said it was not just a Home Office costing of £1.7 million per life; it was following a Treasury model, a Department of Health model, or a police model. I find those savings a bit fanciful. I can understand why the cost is paid by the taxpayer, the Chancellor and the Government, but I do not understand how the Government gets the benefit of £1.7 million savings, on average, if I am not killed. All I am saying, Home Secretary, is I think those cost saving are fanciful. Can you elucidate today?
Mrs May: I am very happy to send something into you that would go into more detail, but the point is there is an overall cost. We are talking about 1,000 to 2,000 lives being saved. That is the figure that comes through. Quite a lot of work has been done by the Home Office and the Treasury in terms of looking at that figure, and how that figure comes out. If somebody is killed, then there is an immediate cost to the state of what happens around that death. That can be quite considerable in terms of the cost of investigation, and so on and so forth.

Q1197 The Chairman: The benefit to the family of someone not being killed can be estimated in millions or hundreds of millions of pounds, they would feel, but the cost to the state of someone being killed is certainly not £1.7 million. I read through the figures again, and I cannot, for the life of me, get my head around how the Government thinks there is an individual saving to the taxpayer of £1.7 million on average for someone who is not killed.
Mrs May: There is an initial saving in relation to the case. There is then, potentially, a saving depending on the circumstances of the family, as the death of one individual might actually throw the family onto the state. There are all sorts of factors that could be taken into account in relation to this.

Q1198 Dr Huppert: This is essentially the question I put to Charles Farr last week. If the Home Office figures about projected savings, whether it is lives or financial, have much backing, you can presumably point to evidence over the last 10 years of the lives saved and the amount of money that has been saved. I think the Home Offices figures are £6 billion as a projected benefit over the next 10 years. How many lives have been saved in the last 10 years using communications data, and how much real money—as opposed to the lives saved—has been brought to the Government as a result of communications data in the last 10 years?
Mrs May: It is difficult for us to say that, because I am not sure that we have actually been accumulating that data in the way that you would require it to be accumulated in order for me
to answer that question. We have been able to make some estimates from cases of how many lives might have been saved, but we have not been sitting there in the Home Office totting up these things in the expectation that I might have to answer a question at a joint scrutiny committee.

Q1199 Dr Huppert: I am just trying to understand, because if the estimates are accurate going forward, presumably one would expect them to be based on the evidence that we have already accumulated. If they are not based on past evidence, which is what I would have expected, where do they come from? Will you, if the Bill ever comes before Parliament, be able to justify the estimates based on historic data by that point.

Mrs May: These sorts of issues about the cost-benefit of the programme should come through in the impact assessment that will be done and will be presented to Parliament. So Parliament will see what the various figures are.

Q1200 Dr Huppert: They have been presented to us, and what we are saying is that there is not the evidence to back up the impact assessment that was produced with this draft Bill. Can you be sure that you will have sufficient evidence by the time this gets any further, if it does?

Mrs May: I am able to reassure you that we will be able to show why we have come to those figures. I recognise, as a research scientist, you want absolutely hard evidence on everything. It is not necessarily the case that for every kidnap that has been stopped, so a life has been saved, the police officer or somebody has sat down and said, “Well, that has saved the state X amount of money”. That is what I am trying to say. Obviously, there are some estimations in here, and so forth. So we can show you how we have arrived at the figures. I am not sure they would satisfy your eagerness for absolutely hard, concrete evidence.

Dr Huppert: It would be helpful to see where the estimates do come from. If you can send them to the Committee, that would be fantastic.

The Chairman: I am just amazed that Home Office accounting officers have been able to put one over on the Treasury.

Q1201 David Wright: Home Secretary, in the foreword to the draft Bill, you say that you will consider the views of this Committee and the Intelligence and Security Committee carefully, before introducing the Bill later in this session. Now, your officials have told us that they do not expect royal assent for this Bill until 2014, so could you tell us whether the Bill is going to come forward in this session, what your timetable for implementation is, and whether there is coalition agreement on this Bill?

Mrs May: The timetable that we have set is that we would be able to receive the evidence from this Committee and the ISC in time to introduce before the end of this session, but to carry over into the next session.

Q1202 David Wright: You expect this to come in to this session

Mrs May: I am expecting it to come in to this session. Now, obviously, that slightly depends on the new evidence that we get from the committees, and the extent to which we need to look at the draft Bill in relation to the reports that come through from the two committees. But that would currently be my expectation.
Q1203 Craig Whittaker: Home Secretary, I know we have briefly touched on this already, but our evidence does show that, despite assurances from the Home Office, CSPs definitely do not feel as though they have been consulted widely on the draft proposals. Do you believe, going forward, an opportunity will be taken to consult with not only CSPs but perhaps civil liberty people as well?

Mrs May: As I indicated earlier, we have discussed this Bill with a range of people, and we have been talking to CSPs about the nature of CD and about what we need to do, and, obviously, more latterly, about the specifics that have been in the Bill. We will indeed continue to do so. We want to work co-operatively with the CSPs, so it is not in the Home Office’s interest not to talk to them, and we will continue to talk to them. Obviously, as we get closer to introducing a Bill, through the discussions on that, we will be able to talk to them in more detail.

Q1204 Michael Ellis: Home Secretary, I just wanted to, if I may, just come to the nub of some of the issues, because I see the time is passing. Would you agree, in a nutshell, that this is a Bill that has been subject to some grossly inaccurate reporting? The measures that are proposed in this draft Bill have not been very accurately transposed in the media. Various names have been ascribed to it that imply, for example, intrusions that the Bill does not include. But would you agree, in a nutshell, that this is a Bill that, if enacted by Parliament and given royal assent, will catch criminals and save lives? Can you give some reassurance that the police that we have heard from, and no doubt the senior officers you have heard from about this, are convinced that this is the case?

The Chairman: I think you just have to say yes, Home Secretary.

Mrs May: I am very happy to say yes. I think there has been misreporting; I think there has been misunderstanding from the public. There have been lots of references from members of the Committee to the public having concerns about this. I think the vast majority of the public want the law enforcement agencies and the police to be able to do exactly as Mr Ellis has said, which is catch criminals and save lives. The first duty of the Government is about protecting the public, and that is why I think this Bill is so important. I think you will have heard of its operational importance yesterday, from Sir Peter Fahy and others.

Q1205 Lord Strasburger: Home Secretary, is it the case that one or more of the senior Home Office officials who are trying to drive this Bill through Parliament are employees or former employees of the security agencies.

Mrs May: We never comment on that.

Q1206 Lord Strasburger: If it were the case, how appropriate would it be for them to be based inside the Home Office, promoting the security agencies’ agenda in pressing for massive increases in state surveillance of citizens, in a way which significantly changes the contract between the state and its citizens?

Mrs May: As I say, I do not make any comment about individuals in relation to the security service, or any of the other security and intelligence agencies. It would not be appropriate for me to do so. Everybody who is working on this Bill is doing so because this Government believes that it is important that the police and the other agencies are able to continue to have the powers that they have today to do as we have discussed earlier, which is to save lives, in a
new technological environment. I understand that the police estimate they get 30,000 urgent requests for communications data per year, and they estimate that they save lives in 25% to 40% of those cases. I think that matters to the public.

Q1207 The Chairman: Home Secretary, as we come to the conclusion of our session with you, I think the Committee would conclude that there seemed to be some considerable movement from your officials between their last evidence session and the first one. As one of our colleagues commented, they had read the body of evidence, and they seem to be willing to be more flexible in how the Bill was drafted—as you have been today—and in some of the outside organisations and public authorities who may be attached to the Bill. Depending on the conclusions of the two committees looking at this Bill, Sir Malcolm’s and this one, are you willing to accept that you might have to do quite a bit of rewriting of the current draft Bill in order to achieve the aim?

Mrs May: I am not able to say how much rewriting we would look at for the Bill until I have seen the reports of the two committees. However, I hope you will have seen from what I have said today, and indeed what officials have said recently, that we recognise that there are some areas in particular where the interpretation of what has been drafted so far is not what we intended, and therefore we need to look at those areas.

The Chairman: I think the Committee would find those remarks very helpful, and perhaps some of the misconceptions we have had have been because the Home Office initially gave the impression they wanted far too much material. As we narrow down what it seems the police and the security services want, and indeed what you want, all of us may be better able to reassure the public. Home Secretary, my very final point is this: it is Halloween, and on the day of Halloween a Home Secretary who is suffering from a heavy cold, or possibly flu, is allowed to put honey and hot water in her large malt whiskey, which I strongly recommend you have tonight.

We are very grateful to you for coming. We are grateful that you have managed to endure over 90 minutes of questioning, despite your heavy cold. We are grateful for the information we have received from you. We will get one or two other things in writing, and we do firmly intend to continue working as hard as we have done over the last few months and over the recess; I want to put on the record that when the Commons was here, Lords came back as well, so we could have meetings. We firmly intend to deliver on time, if we possibly can. Thank you, Home Secretary.