CORRECTED TRANSCRIPT OF ORAL EVIDENCE To be published as HC 479-v

HOUSE OF LORDS

HOUSE OF COMMONS

MINUTES OF EVIDENCE

TAKEN BEFORE THE

JOINT COMMITTEE ON THE DRAFT COMMUNICATIONS DATA BILL

DRAFT COMMUNICATIONS DATA BILL

TUESDAY 4 SEPTEMBER 2012

Professor Ross Anderson, Professor Sadie Creese, Professor Peter Sommer and Glyn Wintle

Evidence heard in Public Questions 330 - 416

USE OF THE TRANSCRIPT

1. This is an uncorrected transcript of evidence taken in public and reported to the House. The transcript has been placed on the internet on the authority of the Committee, and copies have been made available by the Vote Office for the use of Members and others.

2. Any public use of, or reference to, the contents should make clear that neither witnesses nor Members have had the opportunity to correct the record. The transcript is not yet an approved formal record of these proceedings.

3. *Members* who receive this for the purpose of correcting questions addressed by them to witnesses are asked to send corrections to the Committee Assistant.

4. *Prospective witnesses* may receive this in preparation for any written or oral evidence they may in due course give to the Committee.

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

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 et cetera. 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 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 to not just 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 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.