Science and Technology Committee

Oral evidence: Investigatory Powers Bill: technology issues, HC 573

Tuesday 10 November 2015

Ordered by the House of Commons to be published on 10 November 2015.

Watch the meeting

Members present: Nicola Blackwood (Chair); Victoria Borwick; Stella Creasy; Jim Dowd; Chris Green; Dr Tania Mathias; Carol Monaghan; Graham Stringer; Valerie Vaz; Matt Warman

Questions 1-90

Witnesses: **Matthew Hare,** Chief Executive Officer, Gigaclear, **John Shaw**, Vice President, Product Management, Sophos, and **James Blessing**, Chair, Internet Services Providers' Association, gave evidence.

Q1 Chair: Can I welcome the first panel to the introductory session of our new inquiry into the technology aspects of the Investigatory Powers Bill? We have launched this inquiry specifically as pre-legislative scrutiny to assist colleagues in understanding some quite knotty technological aspects of the Bill. It is important that the non-scientists and non-technologists in Parliament understand them so that we can scrutinise the Bill as it goes through Parliament. I hope that the witnesses before us will be patient and speak in plain English as we try to get under the surface of this Bill. I have a briefing from the Home Office which describes the intentions and nature of their Bill. They say that the Government will not ask UK-based CSPs to keep third-party data which crosses their networks from overseas companies, that Ministers have rejected the idea that overseas CSPs should be forced to meet domestic communications retention obligations, that the draft Bill will not introduce any new powers to ban or restrict encryption, and the only new power proposed in the Bill is the retention of internet connection records. Does that chime with your reading of the Bill?

Matthew Hare: No.

Chair: Would you like to start, Mr Hare.

Matthew Hare: I run an internet business which provides, builds and operates new fibre networks, so we are an access business providing connections to homes and businesses. Before that, I ran internet services businesses where we bought infrastructure from third parties to deliver services both to residences and businesses. I have also run businesses that wrote software that worked over the internet to allow people to do e-commerce and provide services.

There are quite a few things I would be concerned about. The first is the sheer quantity of data that currently flows across the internet and the rate at which it is accelerating. The first problem I would have as a business that provides internet access is that we now provide internet access at much faster speeds than the UK average. To take a typical 1 gigabyte connection to someone's home, over 50 terabytes of data per year are passing over it. That is a normal connection, so that is 15,000 gigabytes of data a year. If you say that a proportion of that is going to be the communications data—the record of who you communicate with, when you communicate or what you communicate—there would be the most massive and enormous amount of data that in future an access provider would be expected to collect and keep, if it received a notice. I accept that you would have to be a notice provider, but it is the most massive amount of data.

A normal network would assume that between 2% and 5% of that total data content is the bit that this Bill may or may not be interested in, so you have the most massive amount of data per customer that you will need to gather and hold, pretty much in real time. That is the first problem I have with what they are proposing. The indiscriminate collection of mass data across effectively every user of the internet in this country will have a massive cost. Fundamentally, I would question whether you are going to meet some of the goals put into the foreword of the Bill as to why this is needed. I think it unbelievable that a terrorist organisation or a serious criminal will not already be encrypting all of their content across the internet in one form or another. All you will do is create a massive database of who uses the internet for what and when, to be stored across a whole range of different service providers to make sure you have the content available, and I would question whether keeping that secure and safe is always going to be the case. As some people have said, if Mr Snowden managed to publish what the NSA are doing, how on earth can the rest of us guarantee that any data we hold will always be safe?

Q2 Chair: Mr Shaw, Sophos is in the job of keeping data secure and safe. We have just heard from Mr Hare his concerns about the volume of data, the cost of keeping it secure and whether the Bill will meet its goals of law enforcement and tracking terrorist activities, but also about the impact in terms of encryption. Do you share those views?

John Shaw: Yes. We are in a slightly different position. As you say, we provide security software. We are the biggest company in western Europe to do that. We are UK-based. We do about £300 million a year and export pretty much all of that. We have some concerns related to our UK-ness. There are some things about UK-ness that are a bit different in the Bill. I certainly share the concerns Matthew mentioned around the amount of data that would need to be kept by service providers. There is also an interesting question as to what exactly a service provider is. Some of the definitions are quite loose. As far as I can see, it is not explicitly stated but there has to be implied, at least by other legislation, a strong requirement on service providers to protect the data they are keeping. There would be a huge amount of very sensitive personal data that could be used by bad guys. The TalkTalk example is an unfortunate recent one that demonstrates that it is very hard for companies to protect everywhere the kind of data they keep about people, and this would be a requirement to keep a huge amount of further data.

There are some attempts in the Bill to distinguish between the delivery mechanism of the data and the content itself, but in reality it is very hard with most forms of communication

to make such a clear separation. You end up having to keep an awful lot of the data, even if you are not keeping the content, and that data can be very meaningful for someone wanting to use it for nefarious purposes; for example, which bank someone uses would be very obvious. There is a lot of data in the way in which web communication would happen that gives you a bunch of clues as to the content going in there and it is very hard to separate those things. There are a lot of concerns about that.

We would also be concerned about what constitutes a service provider. There seems to be an implication that UK-based companies will be treated differently from non-UK-based companies. I think you mentioned that in your introduction. For UK-based companies that serve non-UK customers, there is evidence from examples of things happening to Microsoft right now in the US that can undermine the confidence of non-UK customers, whether they are businesses or consumers, buying something from a UK business, if they feel that their data will somehow be spied on or used for nefarious purposes. That is the second area.

The third area is around the definitions. In the Bill itself there are definitions of telecom service, service providers and service operators that attempt to be very broad so as to be future-proofed, but are therefore very broad in the sense that you can define almost any form of software or communication these days as being a telecom service. I have concerns over exactly how far the powers will go. They could be interpreted as going a lot further than I believe is the intention.

Q3 Chair: Mr Blessing, has Mr Shaw identified the key problem with the challenge between future-proofing and establishing clear definitions? He has identified that your trade body, as service providers, are not being clearly defined, in his words, within the Bill. How could you future-proof that? Do the concerns that have already been outlined represent yours?

James Blessing: Yes. We are very concerned. The whole idea of an internet connection record does not exist as far as internet service providers are concerned. We do not have an internet connection record. We do not store information about what our customers do online in this particular way. It is not clear from the Bill what constitutes a connection record. There are comments in various places about recording just the first part of a web URL, but that is not in an internet connection record from the basic definition, which is a communication between two end points. Those two end points are not necessarily a website. It might be something in front of a website, or it might be a service. If you want to get at the URL someone is visiting, you need to open the packet, inspect it, take information out and then throw data away, which makes the whole processing of those records even more complicated and prone to mistakes. If somebody is being clever with the URL, you may be taking more or less data than you intended to take. It then becomes a big problem when you are trying to aggregate records across multiple service providers.

As the wording of the Bill stands, it talks about individual notices being given to service providers about what they should take and the inability of those service providers to discuss those records with anybody else. That is understandable from the security point of view, but internet service providers around the world have to co-operate with each other. The internet is not a single network; it is multiple networks made up of little networks that talk to each other on the border. Unlike many industries, there is very close co-operation between individual service providers on technical issues, because a technical issue at a

border between two networks affects everybody's customers, so you spend a lot of time discussing those things.

The way the Bill is at the minute means there is not a clearly defined interception programme that service providers can sit down and discuss to work out the best technical solution to provide what the security services want going forward. It also means that, potentially, as things change, those notices will change. If there are some big changes in the next five or 10 years, a big service provider could have three or four different retention notices served on them. That is three or four big projects to change the way they are recording data. That leads to a situation where no one is getting the best benefit from sitting down and going through this from day one to see what they are trying to achieve in terms of interception.

The Bill itself is increasing what service providers have to do. Pretty much every single service provider understands that law enforcement is trying to deal with the changing environment. Unfortunately, it is a struggle to find a solution that will work. I do not think there is a solution where we can say, "This is the solution going forward."

Q4 Chair: But do you have recommendations in terms of clearer definitions?

James Blessing: Yes. It would be our preference that the Bill includes very clear definitions of everything in it, a method for those to be updated with reference to the Technical Advisory Board, which is already in the Bill, and then a statutory instrument to make those changes. You would have technical oversight to make sure the changes make sense and, if there was any political or policy impact of the changes, both sides of the argument are captured and you can divorce what is a technical problem from a policy issue.

Q5 Jim Dowd: I detect a certain lack of enthusiasm for the Bill on your part. Mr Hare and Mr Shaw, you have already mentioned this: how feasible would it be for ISPs and communication service providers to comply with the additional measures outlined in the Bill?

James Blessing: The easiest way of saying it is that they will find it very simple if they are given an infinite budget. If you give me lots of money, I can do this for you.

Q6 Jim Dowd: That is very practical. Thank you.

James Blessing: The Bill appears to be limiting the amount of funds available to a figure we do not recognise as one that would be suitable for the entire industry to be able to do it. There is talk of restricting it to certain organisations, so that may be why the figure is lower than expected. Part of the issue is that end-to-end communication is very rare. In an internet connection between person A and service B, there tend to be several things in between. If you are using your computer at home and you have a wireless router, everybody in your house shares the same IP address, so I can say that somebody at that house accessed a service, but I cannot tell you which of the people at that particular location was accessing it.

Q7 Jim Dowd: Surely, that is no different from an individual using somebody else's computer.

James Blessing: I am just going through it. At the other end of the conversation, where you are talking to a website or service, it might be shared. A number of big companies that do content distribution run the services on their servers, so you have things like the BBC and NASA on the same network, and you do not know whether that person was talking to NASA or the BBC. All you see is a connection from that router to a server that has some things on it.

Q8 Jim Dowd: But that is no different from an itemised phone record. All you know is that that phone call took place. You do not know who made it, so it is no different from that.

Matthew Hare: There is quite a big difference, in that the fundamentals of telecoms—making phone calls—rely on collecting billing records throughout the network in order to assemble them and bill the end user. That does not happen in IP networks, so there is not the same mechanism built fundamentally into the infrastructure of data networking as there is in voice telephone calls. The analogy that it is the same as telephone calls is wrong.

Q9 Jim Dowd: Essentially, you are saying that the Bill is not feasible at all for internet service providers.

Matthew Hare: From my point of view, running an internet service provider, two different things are being talked about in the Bill. The first is the individual interception warrants of various types and regularising that regime so it is the same warrant from whatever source it comes. That is probably not a very good summary. It does not matter whether it comes from Scotland or England, or from the Ministry of Defence or the Metropolitan Police; it is the same process. To me, that seems perfectly workable, but that is a named warrant, in the same way as we have them at the moment. The regularisation of that part of interception seems pretty straightforward and sensible, from what is being proposed. Where I have problems is the idea that we should as an industry be tracking what everybody is doing all the time regardless. The fact is that 99.999% of their activity will be completely innocent, so it is a massive dragnet on the basis that at some point in the future you might be able to reconstitute data that might mean you could find out something about somebody in the past. That is where I have huge problems with what the Bill is proposing.

There are some secondary issues, which I am sure John will talk about. If I was a software business, which I now am not, developing software in the UK, and this Bill was in legislation today, I would be very worried that my customers would not buy my software any more if it had anything to do with security at all. It is difficult to see any type of software that would not have something to do with security. I would be worried that a back door was built into the software by the Bill that would allow the UK Government to find out what information was on that system at any point they wanted in the future.

Q10 Jim Dowd: What you are basically saying is that this is perfectly feasible as long as you are not asked to do anything more than you are doing now. Beyond that, it becomes infeasible.

Matthew Hare: No. I would support James in saying that what has been proposed in this Bill they have already managed to do in Chi**na** with the firewall. If we did the same thing here in the UK, you could capture all the information about what is going where, when and to whom.

Q11 Jim Dowd: On cost, Mr Blessing says that you need an infinite budget.

Matthew Hare: It will be less than infinite, but it will still be pretty big.

John Shaw: Everything is less than infinite.

Q12 Jim Dowd: Who should pay?

Matthew Hare: The taxpayer will pay in the end one way or the other, so the citizens of the country will end up paying for being spied on.

Q13 Jim Dowd: But not in their role as taxpayers; they pay in their role as customers of the various ISPs.

Matthew Hare: Yes.

James Blessing: Even if the hardware costs are met up front, which is the established method for cost recovery, the ongoing costs of storing and looking after that data—the cost of powering servers with hard discs spinning—will still have to come out of individual end-user customer price rises. They will not be massive, but they will still be price rises.

Jim Dowd: But customers pay for everything in the end in all businesses.

Q14 Matt Warman: I declare an interest. I am on the Joint Committee looking at the Bill. We are already paying to be spied on because that is how we fund the secret services, but that is a separate issue. You seem to be conflating two arguments. You say it is not like a phone call because the billing mechanism requires you to track one phone call in order to make people pay for it. That seems perfectly logical. You then say that because there is not a built-in billing mechanism it is not okay to have a similar dragnet for this kind of data. They seem to me to be two very different arguments. If it is okay to have the dragnet for phone calls and it happens to be involved in billing, surely it is okay to have the dragnet for the web, and who cares whether it is involved in billing.

Matthew Hare: The web is not a single application. That is the fundamental problem I have with the comparison. Think of a teenager on their computer at home. They are playing a game where they have communicated with their friends using something called Steam. That is not a web application; it is an application that sits on your computer and

talks to other users over the Steam network. They are broadcasting the game they are playing using something called Twitch, which is another application that also sits over the top. They may well also be doing a voice call at the same time with their friends, shouting or screaming, "Careful, because there's grease round the next turn," or whatever they happen to be doing, and that is another application running. All those applications are running simultaneously. They are different applications using different servers with different services and different protocols. They are all running concurrently on that one machine. That one communication is made up, just in that example, of four different services running in parallel. At any time one of those services could drop in, drop out or be replaced.

On a webpage, if you look at the information at the bottom of the browser and what is happening as a webpage is loading, you will see that that webpage is made up of tens, or many tens, of individual sessions that have been created across the internet just to load a single webpage. Bluntly, if you want to find out what someone is doing you need to be tracking all of that data all the time. On a one-to-one basis, that is what happens right now; we do something called port mirroring where everything that is delivered to a customer can be delivered to a third party, obviously with the right credentials, but that does not mean that we are trying to break it down individually and store, track and log all of that information and keep it available for someone else to look at.

Q15 Matt Warman: But your argument seemed to be that it was somehow ethical to do it for phone calls and unethical to do it for the internet. Now you are just saying it is difficult to do it for the internet.

Matthew Hare: I think the ethics question is exactly the same in both cases. I agree with you.

Chair: We are here to talk about the technical aspects of the Bill. There are two other Committees that will look at the ethics.

Q16 Stella Creasy: Actually, I want to follow up on that. One of the things you and Matt talked about is that it is a dragnet. The current system, particularly on IP addresses, means that you would have to capture a lot of information to find a person of interest. I would be really interested to get your views on whether one of the answers, both in terms of the cost and the ethics, is the move to IPv6. Right now we are fishing in a big pool, but IPv6 would allow you to look for a much more specific IP address. It is my understanding, for example, that Parliament has two IP addresses for all the thousands and thousands of users. If you were to look for a person of interest in Parliament, all our data would be captured in that dragnet. A move to IPv6 would help you to be much more specific if there was a person of interest that maybe the security services wanted to look at.

James Blessing: IPv6 would make it a lot easier to find people, which is fantastic. Adoption of IPv6 is a bit of a challenge.

Q17 Stella Creasy: Could you talk us through that, because it is a very technical area? IPv6 would give everybody an IP address.

James Blessing: Yes. Many years ago, IPv4 was the only choice you had. Vast swathes of it were given out to lots of different people and everyone thought, "We'll never need more than 4 billion addresses." It turns out that we do. In 1997, people started working on IPv6 and how we could change the existing system to one where, until we moved planet, we would have plenty of address space. That is fine. That works. We have it built and it works in lots of equipment. Unfortunately, with IPv4 we have been very clever. We have been doing things like NATs so that people share address space, which has pulled back on the demand to move to IPv6.

However, in the last two years, because we ran out—we really did run out this time—there has been a push to move to IPv6. There are a number of providers who are 100% IPv6. BT were at less than 1% last time we looked; I think Sky managed to get to 25% last month. If everybody was on IPv6 it would make life easier, but you would still have to capture everything because it is not tied to an individual. IPv6 works slightly differently, in that a single device can have multiple v6 addresses for doing different things, and it changes its address much more frequently. While it would make it easier to identify the end user, you also have more data to go through in the first place, so it is swings and roundabouts.

Q18 Stella Creasy: My understanding is that, for example, where I was using an IP address and somebody else was using an IP address, if the police were seeking to track somebody through that dragnet it would be like spear fishing rather than just putting out a net and casting for every single bit of data.

James Blessing: It would be easier.

Q19 Stella Creasy: Have you had any dealings with American companies? In America they have subsidised the move towards IPv6. My understanding is that American agencies have made it a contractual requirement for some companies to move up to IPv6, partly because it makes some of this easier.

James Blessing: Yes. There are contractual requirements in giving anybody any money. Anyone who wants a Government contract has to provide IPv6. I think ISPA asked the Government to consider that about 12 or 13 years ago.

Q20 Valerie Vaz: I was interested in your opening remarks about the Bill. Could I ask you to clarify? Are you saying that this Bill is not necessary because you can do whatever the Bill wants you to do anyway?

Matthew Hare: At the back of the Bill is a list of all the things they are going to repeal and replace with the Bill. It is a wide range of different bits of legislation. If today we as a company received a notice requiring us to intercept traffic to a particular IP address, we could do that, as could pretty much any ISP in the UK. I cannot speak as to communication service providers, but the Bill appears to widen the net to include them. Could Twitch deliver this information to you if they were served with a notice? Probably, but I have no idea.

James Blessing: Most modern hardware has been built with the American market in mind and, therefore, most modern hardware has some form of law enforcement ability to copy a port. It is a bit crude, but basically it says, "All traffic from this destination needs to go here." You then need to do some more work, but you could capture that traffic quite happily.

Q21 Valerie Vaz: Mr Shaw, did you want to say something?

John Shaw: I think you have covered it. The crucial difference with the new Bill is the requirement to hold 12 months of data on everyone all the time. What Matthew was saying was that in response to a particular demand you can track data for a particular situation, but that is very different from the requirement to capture 12 months' worth of data. That is very new and different in this Bill. It is not just the cost of the data; the exposure of everyone in the UK's data to people trying to hack it to do bad things with it is a very meaningful difference.

Q22 Valerie Vaz: You touched on data. Are the differences between data and content blurred in this Bill?

John Shaw: Incredibly blurred—in real life. It is not the Bill's fault; that is the way things are. That is another place where the telecoms analogy does not really help us very much. In a phone call there is a number you dial and then there is what you say when you speak. In terms of communications over the internet, as Matthew was describing, a lot of the time the data going back and forth is not even what two people are generating between each other; it is a whole bunch of software and services in between sending communications back and forth. What is content, and what is the delivery mechanism and the destination? There is a danger that you would end up having to capture virtually everything in case something within that could be defined as one versus the other.

Q23 Valerie Vaz: That is not clarified in the Bill.

John Shaw: No.

Matthew Hare: The Bill talks about there being, effectively, three layers: stuff that is clearly the address; stuff that is clearly content; and stuff that could be one or the other. The Bill talks about those three different things and how you need to treat them differently. I accept that it does. The problem is that the real world is a bit tricky, and it will be different tomorrow from what it is today.

Q24 Valerie Vaz: In reality, there is no difference between the two.

Matthew Hare: For some things it is very clear. If you are watching a movie on Netflix, receiving that movie is clearly content. If you happened to be resizing your screen you might be passing code back to Netflix about something you wanted to pass across the internet, because every time you resize your screen it sends control information back to Netflix.

John Shaw: Which is a communication.

Q25 Valerie Vaz: To take the 16 year-old hacker, TalkTalk say it is okay; it is just data, not content. That is not true. Effectively, a 16-year-old hacker can get into all our data and our content.

James Blessing: We are conflating two things. Once you have captured the communications data it becomes content. You capture it and then you put it into a database and it becomes information, because it is content about the communication. Once it becomes part of the database it becomes content and it becomes very attractive to anybody who wants to use it for nefarious matters, or just to have some fun.

John Shaw: The fact that you bank with HSBC, which you can deduce, in anyone's definition, as communications data, is then meaningful information about you, which will have to be stored.

Q26 Valerie Vaz: Were you aware of the handling arrangements for bulk personal databases that came into effect on 4 November?

Matthew Hare: Which regulation?

Valerie Vaz: It came into force on 4 November this year just as the draft Bill was published. It is about the handling arrangements for bulk personal databases. Are you not aware of that? I am not expecting that you should be.

Q27 Chris Green: Mr Shaw, will the Bill either by its measures or by drawing attention to available investigatory powers drive more activity offline, or perhaps overseas?

John Shaw: That is a good question. I think Matthew has referred to it already. Any actors, whether they are terrorists, cybercriminals or whatever, are already using mechanisms in the vast bulk of cases that would not be interceptible under powers in this Bill or previously, so I am not sure it will drive any more of them to use encrypted communications mechanisms than are already doing so.

The one area where I would have concern—Matthew alluded to it—is that you could interpret some of the definitions in the Bill as meaning that a UK-based company is obliged in some way to hand over more data than a non-UK-based company. That runs the risk of putting UK-based companies at a disadvantage when trading with non-UK citizens, who would then be suspicious of using the UK-based company.

Matthew Hare: Or even trading with UK citizens. Why would you buy something from a UK company if you thought it might have a back door that it might not have if you bought it from a Russian, Venezuelan or Chilean company?

John Shaw: Russia might not be the best example.

Matthew Hare: I don't know.

Q28 Chris Green: Would the more sophisticated criminals still be able to bypass these measures, but many others who did not know these techniques would carry on and you could still catch them out?

John Shaw: Encrypted email traffic is incredibly common, and some level of encryption would be pretty much the default these days.

James Blessing: The issue is that you are not necessarily pushing experienced cybercriminals or people who have nefarious connections to encrypt things. You are more likely to push people who have nothing to worry about to use encryption more often, which might be a good thing from a safety point of view. It might be good if more people paid more attention to their security.

John Shaw: Although it would be a shame if we then stored all that data for someone to access separately.

Q29 Chris Green: Mr Blessing, you said that there were different networks. Would there perhaps be a chilling effect between those networks if the Bill went through as it is, or, because of the perception of what it would do, would other networks relate to it differently?

James Blessing: It will have an effect. We are not quite sure where it will go or what the effect will be, but it comes down to this. Where a company has a choice between a UK company and an Irish one in terms of service, if UK law, in their perception, even if not in reality, is stricter, or more likely to expose their details, they will choose the safer option, especially if they are risk averse. The more risk-averse companies will take it into account. They may not take it into account on the basis of a real level of danger but a perceived level of danger.

Q30 Chris Green: Mr Hare, you touched on investment—whether a UK company investing in the UK, or perhaps an overseas company. If we go down this route, will it cause a problem with investment in software companies in the UK?

Matthew Hare: I definitely believe it would if all the provisions in the Bill as currently written were put into law, which I certainly hope will not be the case. It will definitely affect both hardware and software companies based in the UK, potentially even service companies like lawyers. Why would you want to be based in the UK if potentially the Government have given themselves the right, frankly, to hack all your equipment with the connivance of your service providers? From reading the Bill, it appears to me that that is the right it gives the Government.

Q31 Chris Green: In terms of investment and in terms of companies developing software here, there would be less and, therefore, less ability to access it in future.

Matthew Hare: It goes beyond the companies who are developing the hardware and software. The UK relies on the information industries in their broadest sense, from financial services through legal to software and gaming; it affects everyone in the information industry. If we make it appear that this is a worse place to do business, because of some rights that, as far as most of us know, the Government never take up—

but we will never know because we are not even allowed to talk about it—it seems to me a massive own goal.

Q32 Victoria Borwick: How anonymous are the users of Tor and the darknet, or not? Would that undermine the effectiveness of the Bill, or, in view of what you said, do you think people will leap over and do something else?

James Blessing: One thing about Tor is that it needs exit nodes to work. Some people enable the exit nodes and some people do not. Certain people's data is exempt from being captured, but if your data is being captured and you were running an exit node it would look like you were doing the browsing. You would take on the appearance of whatever the person using Tor was doing. Tor works basically by hiding from each other who is using it; they do not know—they have no idea. You will see upstream nodes and other people who are connected, but you would have to hunt around those locations to find out who they are talking to. Tracing it back becomes quite difficult.

John Shaw: The short answer is no, you cannot tell who they are.

Q33 Victoria Borwick: Would the police be able to? The point of all of this is to tackle crime, isn't it? That is what it is all about.

James Blessing: Tor causes an awful lot of problems because of the way it operates. It is very difficult to trace it back, but this Bill would not help. It would tell you where the exit node was and the nodes it is connected to and you could follow it back, but it could quite easily hop outside jurisdiction into Switzerland, France, the US or Peru. You would then lose the ability to trace it unless you had very tight law integration with those particular countries.

Q34 Victoria Borwick: What about general use of the darknet and that side of things?

John Shaw: From the point of view of our area of expertise, Tor is very commonly used by cybercriminals, precisely because you cannot tell where they are sending stuff and, therefore, who they are.

James Blessing: There is not a single darknet; there is a series of different—hidden— bits of infrastructure where people use other infrastructure to hide. It is not as simple as saying that if you crack Tor you have cracked it all. People will just move to something else very quickly.

Q35 Victoria Borwick: I am slightly concerned that in a way we would always be playing catch-up, wherever we are on the darknet. If people cannot use this or that aspect they move on. It is an evolving technology.

James Blessing: You would be better employing ITAC guys to work with the police to target individuals. It is a lot easier to go after a person than to try to use technology. You will still need technological tools to help and aid that person, but it is much better to go after the individuals rather than the technology.

Q36 Chair: Can you talk me through the enforcement implications for online transactions with things like cryptocurrencies, bitcoin and PayPal? Would this Bill make a difference? Would it be easy to follow those transactions? Are the communications working in the right way for that? Have I asked a difficult question?

James Blessing: It is not a difficult question. I am trying to think of an answer that will make sense. PayPal is quite easy; it is a bank. At the end of the day, it is a very simple system to follow and trace transactions. Things like bitcoin and cryptocurrencies work on a slightly different principle. The Bill is not going to help you there, apart from being able to point you in the general direction of people using bitcoin exchanges, where they are transferring money between bitcoin and real money and coming back into the real world. That is the transaction point at which you will be able to catch those who are using those exchanges. The point is that people using them innocently will be captured as well as people doing it not so innocently. The Bill itself does not address that, apart from some of the sections that allow the Home Secretary to introduce new technological things and potentially, if it was there, to require encryption to be back-doored. That is probably a bad term.

Q37 Chair: There is nothing in the Bill for back-dooring encryption, is there? There is the existing power, as I understand it.

John Shaw: The introduction makes it clear that there is no requirement for a back door, which is great, because there had been some discussion about that. It is great that there is no intention to have a back door. There is one particular clause, which does not use the word "encryption"—

Matthew Hare: "Bulk equipment interference warrants".

John Shaw: That is slightly different.

Matthew Hare: I do not know whether it is different. You could easily interpret that to enable the Secretary of State to require software and hardware developers to provide back doors.

James Blessing: It might not be the intent of the Bill, but the current wording of it seems to imply that that may be used at a later date.

Matthew Hare: It is chapter 3, if anyone wants the reference.

John Shaw: Bulk interference is a euphemism for hacking, and I guess that could cover just about anything. It does not really restrict what bulk interference could or could not be.

Q38 Chair: You would understand that as introducing an encryption back door.

John Shaw: No, but Matthew might. I would understand it as hacking.

Matthew Hare: I would understand it as giving the Secretary of State the ability to introduce a back door under the law whenever they wanted.

Chair: I do not think that is how the Home Secretary understands it.

Q39 Graham Stringer: Encryption has been mentioned a few times. How big a problem is encryption for the security services and other law enforcement agencies?

John Shaw: Do you mean how big a problem is it for them to encrypt or to decrypt?

Q40 Graham Stringer: Decrypt.

John Shaw: That is probably a question best put to them.

Q41 Graham Stringer: Has encryption got to such a point that it is unbreakable?

James Blessing: No. You can break encryption.

John Shaw: You can always break it given enough time and computing power.

Q42 Graham Stringer: If it is longer than the existence of the universe, it is not a lot of help.

John Shaw: It is rather like the internet budget. With infinite time you can crack anything.

Matthew Hare: Gov.uk is encrypted—the whole Government website is encrypted. I assume that as a country we are encrypting the Government website because we do not want to share that information with third parties.

Q43 Graham Stringer: I understand why things are encrypted. What I am asking is can the security services decrypt encrypted messages, or have we passed the point of no return on that? If we have passed the point of no return, what is the point of this Bill if you cannot get into those messages?

John Shaw: Given enough time, computing power and so on, you can in the end decrypt anything, at least using brute force, which is that you try every possible permutation until you get to it. There are cleverer things to do than that. It depends on the situation. If you are trying to decrypt a target in a particular situation, you probably can, but if you are trying to decrypt everything communicated by everyone all the time, you certainly cannot. It depends on what you are trying to decrypt, and how far you are trying to go.

Q44 Graham Stringer: In a sense this is a side issue because the Bill does not mention encryption. Is it right not to mention encryption?

James Blessing: If you were to try to stop people encrypting things, you would wipe out the ability for people to do transactions online in a secure way. Basically, you would not be able to use online banking, submit your tax returns or read your emails safely, because everything on the wire would be available. Someone could sit in a café and read

everybody's communications. That would be the end of the internet in terms of using it for anything other than watching videos.

John Shaw: Encryption is a tool which is used largely for good reasons by good people to protect themselves from bad people—from things like the TalkTalk hacking incident and so on. If that data was encrypted no one would have been able to do anything bad with it. Encryption is an important tool that is generally used for the good. The danger is that if you restrict the ability to use encryption for the bad, you probably cause more damage to consumers than you would by allowing everyone to encrypt.

Q45 Graham Stringer: My last question is really asking the previous question in a different way. If the bad guys are using encryption and it is very difficult to decrypt, how much point is there in the Bill, even if you have access to that data?

James Blessing: It is because the Bill says it does not want to see the contents of the message but who they are talking to. It is very clear that that is what it is trying to do. The problem is that it is not quite achieving that. It is not seeing the whole conversation but a bit of it—

John Shaw: In terms of the data being stored for 12 months. There is a requirement to store 12 months' worth of data about the communications. We talked earlier about the difficulty of defining exactly what that is, but there is a requirement to store that amount of data. It is a bit different from encryption in that sense. It is really important that that data itself is then encrypted, because that is a whole bunch of very pertinent, personal information about every UK consumer that could be used for bad purposes if it is not properly protected. Part of the cost is not just collecting the data but making sure that it is then super secure—so every ISP has to do it—so that it cannot be used for bad purposes. There may not be enough encryption in the Bill from that point of view.

Graham Stringer: That is interesting.

Q46 Matt Warman: There are quite a lot of points where the three of you disagree about what the terms might mean precisely. It seems to me that, even on Mr Hare's point about whether or not there is a back door, it would still be subject to the double lock with the Secretary of State and a judge anyway. What we are talking about is making sure we get the terms properly defined before we start making accusations about who is allowed to do what at some point in the future. Is that a fair question?

James Blessing: There is a lot of fuzziness in the Bill. I can understand why some of it exists in terms of trying to future-proof it, but some of it is too fuzzy and the interpretation depends on who reads it, what mode they are in now and how paranoid they currently feel.

John Shaw: I want to clarify "back door." I do not have the interpretation that anything in it refers to a back door, with one possible exception. The notion of equipment interference is talked about. It is very vaguely defined, but it is clearly something that happens after the fact. There is no implied request, as far as I can see, that a service provider, however defined, should provide some special access. The onus is still on the security service, or whoever it might be, to try to interfere in some way rather than to allow them access. I do

not think there is a back door in that sense. There is one clause—189—that talks about "obligations relating to the removal of electronic protection applied by a relevant operator to any communications or data." It does not use the word "decryption", but "removal of electronic protection" has some implication there. It is not a back door; maybe it is a front or side door—I am not sure—but a door of some kind is implied in clause 189.

In answer to your original question, it is another example of very loosely defined things. What does removal of electronic protection mean? What does equipment interference mean? What is a telecom service provider? These are either not defined at all or very broadly defined in ways such that you could interpret just about anyone as a telecom service provider, if you are not careful.

Matthew Hare: Which is of course what it says in the Communications Act. Anyone who provides a service to another party is a communication service provider, so in that respect it is consistent.

John Shaw: In that sense, anyone running a network at home could be defined as a private telecom service provider.

Matthew Hare: There is an exclusion at the beginning of the Bill; that is allowed interception.

Q47 Matt Warman: The fact that we are having a Joint Committee, followed by quite a long process is, I presume, the opportunity for you guys to make your collective case and for some of those definitions to emerge.

John Shaw: We hope so.

Q48 Carol Monaghan: A lot of users now are storing data in the cloud and using cloud computing for internet access or emails. How accessible to surveillance or hackers are the data currently stored in the cloud?

James Blessing: They are as secure as the service provider can make them; the last thing they want is someone to compromise it, because they will lose reputation and business. In some cases, they make mistakes and things happen. That is a fact of life. The idea is to try to make that as rare as possible. The data itself is probably technically more secure when encrypted in the cloud than it is on your home PC. I guess that most people at home do not encrypt their own data because they think it is nice and safe. The number of recent cases where Trojans have been installed and have encrypted the hard drive as a ransom method has been increasing. It is always good to have a back-up copy, but it is always good to choose a service provider who encrypts that stuff in the cloud for you, where you have the encryption keys. There are good and bad bits, like everything in life.

John Shaw: In general, companies providing services in the cloud—this is not going to apply to every company all the time—are probably better at securing stuff than the average small business or the average consumer. You could argue that, in general, data becomes safer as it moves to the cloud.

Q49 Carol Monaghan: Is the cloud currently in one physical location? I am assuming by the shakes of the head that it is not. How easy do these locations make it for surveillance or hackers to access them?

James Blessing: The cloud is a short term for other people's computers. I do not mean other people's home computers; I mean servers resting in data centres. In theory, there are data centres and, therefore, a concentration of servers in one location, which technically should make it easier to serve a warrant on the provider in that data centre and do interception to capture a particular thing. The problem is that they are distributed around the world for back-up purposes. You run one in the UK, or more likely Ireland at the minute, one in the US and maybe one in Asia, so that you have very good geographic diversity.

Q50 Carol Monaghan: So my photos could be anywhere in the world just now.

John Shaw: Or in all three places.

James Blessing: Yes. In an ideal situation, you cut the picture up into lots of little bits and then create an extra bit to work out how to put it back together, and make sure some of those are spread out so that if you lose any one of the three you can restore it.

Q51 Carol Monaghan: How burdensome will the Bill be to ISPs when they are asked to provide data currently held in the cloud?

James Blessing: With the appropriate warrant on an appropriate UK-based service provider you can get that information today. In theory, the Bill makes it easier to make that request, because the request should be a bit more consistent, but it is just a request for information at rest, not an interception requirement. An interception requirement makes it more complicated, because a good service provider will encrypt end to end the communication between your machine and the cloud.

Q52 Carol Monaghan: But if the data at rest is not resting in the UK we cannot access it.

James Blessing: Unless it is a UK-based service provider.

Q53 Dr Mathias: Can you explain the relevance and significance of deep packet inspection in regard to surveillance?

James Blessing: We were talking earlier about the fact that you have absolute communications data and absolute content, and a fuzzy bit in between. DPI is the bit that gets you the fuzzy bit in between, because it works out what the communication is. That means taking all the fuzziness and throwing away the bit that may have been content.

Q54 Dr Mathias: Are service providers using it already for surveillance?

James Blessing: Without specifically referencing any service providers, lots of them are and lots of them are not. Once upon a time, when bandwidth was incredibly expensive,

quite a few people had a deep packet inspection box, not to look at the content but to try to slow down content that could take time to be delivered—that was not urgent.

Matthew Hare: It improved the overall quality of delivery.

James Blessing: Exactly.

Matthew Hare: It improved the quality of delivery to customers, so it was delivering the time-critical stuff now and just holding the other bits that could wait a few milliseconds and delivering them later.

John Shaw: So that when you are doing your Skype call you do not get a terrible lag while it is being slowed down because you are downloading the draft Investigatory Powers Bill, or whatever it might be.

James Blessing: Now we have moved on a little and bandwidth is more plentiful and less expensive, most people have thrown away their deep packet inspection boxes, or not renewed them or decided they do not need them any more because they have lots of bandwidth. They can throw bandwidth at the problem, and, if it congests, it is the end user's problem. There are not that many.

Matthew Hare: They are very expensive bits of equipment, because they are working in real time on the information as it flows across them. The data flows across the UK internet now are absolutely enormous.

James Blessing: If you take one particular point in London, at the London Internet Exchange, you are talking about multiple terabytes per second just flowing between networks.

Matthew Hare: What a DPI box needs to do is look in one packet and say, "Okay; that's fine," and look at what is in another packet and say, "That can wait." It has to do that with all the data going through at that particular microsecond.

Q55 Dr Mathias: In your judgment would it increase under the Bill?

James Blessing: Depending on the exact definition of the internet connection records, that is the only way to provide that information. It depends on how much of the fuzziness we need to store. If we have to store things like the URL, or just the first bit of it, we will have to inspect every single packet just in case there is a URL inside it.

John Shaw: For example, to see whether it is a Skype call from one person to another. The service provider who sees only the packets would have to look at all of them to see which one was a Skype call, and that is a lot of packets.

Q56 Chair: Thank you. We are going to close now, but, finally, I want to ask a little about data security. I have heard concerns about bulk data retention, which you have mentioned. We received a document from the NCC group, which made some specific recommendations that would be necessary in a scenario where bulk data retention was introduced. They are quite significant recommendations. They include that all storage of data captured must

employ a minimum of two-factor authentication in order to access or otherwise retrieve information from data silos; that data loss prevention technology is employed at a software and a hardware level in data silos; that robust protective monitoring, including behavioural analytics of the data silos, would be required; and that communication service providers are compelled to establish and participate in threat intelligence sharing agreements, to ensure that they are able to demonstrate ability to action any threat intelligence within a reasonable period of time. That sounds quite provocative to me. I wonder what your response to it would be. You look like you want to say something, Mr Blessing.

James Blessing: They sounded like great recommendations until you got to the threat assessment one. The Bill prohibits you from talking about the fact that you have received a notice to do the retention, so you could not talk about the fact that you were—

Q57 Chair: I think that they are talking about the threat to the security of the data held, rather than—

James Blessing: They are linked. Threats to the way you are collecting and storing the data will be part of the actual notice.

Q58 Chair: You would need to have an environment in which you could report threats.

James Blessing: Yes.

Matthew Hare: There is one clause in the Bill, although I do not think that it is related to this particular bit, which talks about the Secretary of State being allowed to give an exclusion in a specific case from the prohibition on sharing any information at all about the fact that you are involved in the programme. If you were going to do this, that clause should be in the bit about the mass collection of data as well, so that the Secretary of State could at least set up a technical working group that is not the Technical Advisory Board—a working group among the service providers—to make sure that they can work together on things like threat assessments. At the moment, as far as I can see, it is illegal under the Bill.

James Blessing: The standards NCC is talking about are the standards that most service providers follow under PCI DSS, which is the storing of card information for banks. Storing it to those standards is a relatively straightforward process. It should not increase the costs, because it would been have designed like that in the first place. Actually, there will be a minor cost implication, but that is how you should be storing it in the first place anyway.

Q59 Chair: These are recommendations that all of you would endorse.

John Shaw: Other than the last one possibly, which is a bit odd. The other three all make sense. They are describing some more advanced security techniques that many companies do not use today, I would suggest. I guess they have skipped over what they would see as the obvious things, such as having a next-generation firewall, having endpoint security software running on every computer, encrypting the data and so on. It is not a complete

list of the things that you would need to do, but certainly the first three points are sensible things that should be mandated on protecting that data.

Chair: Thank you very much. I am sure that we will follow up with some more specific technical questions. I call the second panel to the table.

Examination of Witnesses

Witnesses: **Professor Ross Anderson,** Professor of Security Engineering, University of Cambridge, **Professor Mike Jackson**, formerly of Birmingham City Business School, **Dr Joss Wright**, Research Fellow, Oxford Internet Institute, and **Professor Sir David Omand GCB**, Visiting Professor, Department of War Studies, King's College London, gave evidence.

Q60 Chair: Can I welcome all of you to our session today? I think you all sat in on our first panel and heard the views that we were receiving. We heard concerns about the amount of data involved in bulk retention, the costs implied for businesses, meeting the stated goals of the Bill and the implications for encryption. Could we start with you, Professor Anderson? Do you share those concerns, or do you think that they are overstated?

Professor Anderson: I agree with much of what the previous panel said. There are significant concerns about the increase of powers that has come with the Bill. The Home Office may technically be correct in saying that the Bill extends existing powers only slightly, but, as Valerie Vaz pointed out, they simultaneously published a number of regulations that extended existing powers in various ways. What we see is an enormous extension of the overt reach of the state. What has happened here, in effect, is that, in response to the revelations by Edward Snowden, we have seen America pull back on what the NSA is permitted to do. On the other hand, things that GCHQ has been doing and that nobody knew about are here being legalised. That may put the two countries on slightly different tracks.

Q61 Chair: I remind everybody that we are talking about the technical aspects of the Bill and how deliverable they are. We have other Committees in this place that are looking at the ethics. Professor Omand, do you think that it is, in fact, the legislation that has changed, or is it the technology that has meant that the volume of the data makes this such a different proposition?

Professor Omand: First, I have to register strong disagreement with almost everything that my friend Ross Anderson has just said. Having heard the previous session, it is very important to realise that most of the questions being addressed are not policy questions or ethical questions, but empirical questions. The question of data and whether the authorities can deal with the volume of data is an empirical matter. The Bill provides for the exception where "reasonably practical", so the Government have given themselves a let-out if it turns out that in some areas this is just too expensive or too difficult. Basically, does the fact that we cannot do everything all at once mean that we should do nothing and not make a start?

Those empirical questions need to be addressed, but they are not ethical questions. We will not find ourselves in a very different position from the United States. The volumes of data on the internet are enormous, but if there is one thing that the unfortunate Snowden revelations have shown, it is that the authorities nowadays are quite good at managing extremely large volumes of data. I would have high confidence that they would be able to derive benefit from the provisions in the Bill, but none of this is a magic bullet. If you are trying to defend the security and safety of the citizens of the United Kingdom, it is done by managing the risk, not eliminating it. This Bill will not eliminate the difficulties of encryption and of large quantities of data—people hiding their evil communications among a variety of different applications—but it will help the authorities to manage down the level of risk. You cannot ask for more than that.

Q62 Chair: How do you respond to the concerns raised by the previous panel about the fuzziness, in their words, of a lot of the definitions in the Bill, which were causing concern about the efficacy of the Bill as a result?

Professor Omand: The main fuzziness they referred to was between content and communication data. The significance of that lies simply in the level of authorisation that Parliament gives for accessing either content or communication data. On the one hand, you are into warrants signed by a Secretary of State and personally looked at by a senior judge. In another part of the Bill, for communication data, you are talking about authorisations by independent senior officers, not in the line of command of the operation but none the less below that threshold. That is where the significance matters.

For most communications, there is a very clear distinction between content, which is the meaning, and the communication data—which device is connecting, in which way, in order to convey that meaning. There may well be some cases, and you could easily think of them, where it gets a little fuzzy. Again, is that a reason for not trying to make a sensible, pragmatic distinction for the very large number of cases where the police service needs access to who called whom to try to track down a missing person, deal with a potential suicide or solve a rape case? It seems to me very evident that the Bill has it right in continuing to make that distinction. Is it perfect? You are never going to get a perfect world, but I would commend that pragmatism to the Committee.

Q63 Chair: Professor Jackson, Professor Omand said that the Bill may not be perfect and that you are never going to get a perfect Bill. Do you have some recommendations for perfecting it?

Professor Jackson: To go back to the discussion that we had, I would be concerned about the amounts of data that were required to be stored. We are talking about this being empirical and whatever. Yes, the data can be stored, but the cost that is eventually put on to people, either through taxes or as they pay for their broadband, might be prohibitive, as our commercial colleagues said, in that it might actually prevent us from exploiting the advantages of broadband. I am also concerned, as our commercial colleagues were, that the Bill contains the possibility that companies who offer end-to-end encryption would be prevented at certain times from providing that facility to their customers.

Q64 Chair: Dr Wright, what is your current impression of the state of the Bill? Do you think that the definitions within it are too vague? Do they need to be tightened up?

Dr Wright: The definitions are too vague. From a brief reading of the Bill, one of my concerns is that previously we had legislation where there were some fuzzy definitions, and we have now learned that the specific interpretation of those terms expands the scope beyond what was believed to be the case; I am concerned that now we have another set of fuzzy definitions that embed the existing state we have got to and allow fuzziness for expansion in the future. That is a considerable concern of mine.

I would have to disagree respectfully with Sir David that there is a clear line between content and metadata. That is one of the key issues coming out of the Bill, particularly when we talk about the meaning of information. Meaning is an incredibly difficult concept in itself, but when we consider the meaning that can be derived from the patterns of communication and the interaction between individuals, as opposed to simply the words that appear within an email, we start to understand that there is a higher level of sensitivity to that data. That means that, when we think about how much cost and effort must be put into protecting that data, it becomes significantly higher. That is core to what I would say are the problems with the Bill.

Q65 Chair: I have heard your analysis of the problems. What would be your recommendations for improving it?

Dr Wright: My main concerns are with mass retention—or bulk retention. I know that there were very careful attempts to remove the word "mass" from the Bill, except in its denial sense. I would certainly want to see a strong understanding of necessity and proportionality in terms of data retention. My understanding at the moment is that there is a requirement for the Secretary of State to decide on necessity and proportionality for retention of data, but, reading around the Bill, it seems that that is every major internet service provider for a period of 12 months. I question whether that necessity and proportionality matches the realities.

Chair: Matt Hancock; sorry—Matt Warman.

Q66 Matt Warman: I was promoted momentarily. Obviously we are in a perpetual arms race, aren't we? To put it in very simplistic terms, the Government are trying to catch up with the bad guys and the bad guys have a vested interest in staying ahead. How do we frame legislation in a way that is both practical now and future-proofed, so that we do not have this debate every six months, six years or whatever? Who wants to start?

Professor Anderson: Perhaps this is an issue Parliament should return to a bit more frequently, because technology just changes too fast. You cannot expect to have a Bill that will last for 25 years unless you have lots of Henry VIII clauses in it and do everything by statutory instrument, which creates problems of its own. The thing that is about to hit us, of course, is the internet of things. The Bill makes some provision for that by talking about things as well as persons, but the true implications of what it means to allow bulk

equipment interference, for example, with road vehicles will probably have to be revisited once people start using autonomous vehicles at scale.

Professor Omand: I agree with the thrust of what you have just heard. It is easy to think about equipment interference that would mean that the car of the foreign intelligence service operative was radiating back where it was. That would be quite convenient. I can imagine that as a rather useful thing, if it were technically possible to do. It does not have to mean the worst case. If we try to interpret this Bill as the worst case we end up in a very bad place, because essentially we will not have the intelligence on which police services and agencies can work.

The communications data definitions are not fuzzy at all; they are actually quite precise. What is not defined in the Bill is metadata, which is a term that the Committee has used itself. The position under the existing legislation is that, if it is not who, what, where or how, it is content, so some of the fancy things that you can do with metadata require a Secretary of State's warrant. I am very comfortable with that, as I know the intelligence agencies are. I would not run away with the idea that definitions in this area of the Bill are that fuzzy.

The answer to your question has to lie in codes of practice. If you try to nail everything down absolutely in the primary legislation, you will be revisiting this in a couple of years' time and passing another Investigatory Powers Act. The answer is to learn from the mistake that the Home Office made over the last five years, which was not to update the codes of practice, so that we, the citizens, knew how the existing legislation was being used. They could have done that, in which case the Snowden case would not have been the shock, horror that apparently it was for many people. Those codes of practice are presented to Parliament. You can insist that they are revised. You could put that in your legislation. There are ways in which the Government at any one time can be quite precise about how it is interpreting them, which will help the judges very considerably. That can then be updated. As to planning because you know in advance that you will have to re-legislate on all of this, Ross is absolutely right—the technology will keep changing.

Professor Anderson: For an example of communications data as used now and defined on the face of the Bill, consider your Google calendar, or whichever calendar you use. On the definition in the Bill, that is communications data. If GCHQ hoovers up everybody's Gmail from the backbone, between Google's data centres, and makes it available, presumably a police officer on a production warrant can find who met whom, when. That is extraordinarily convenient if you are an investigator for the Financial Conduct Authority and you want to know which banker had lunch with which solicitor, or whatever, on what date, but is that what the voters would expect—that their calendar is not content but communications data?

Professor Omand: If that were the case, you would be right, but, as far as I understand it, you would have to check authoritatively that it is not. In other words, the communications data are that you were in touch with the Google server, not what the content of your calendar was. That would indeed be content and would require a Secretary of State's warrant.

Professor Anderson: No. It is related communications data, section 12.

Professor Omand: The example given in the explanatory notes, which I have just been reading, was very clear on this. You could not just go hoovering your way on the say-so of a senior police officer—you would require a warrant for that. If you were doing that, you would know that you were interested in Ross Anderson, in which case you could go for a specific warrant. You would not have any of this argument, because, as you heard from the internet companies a moment ago, they do not have a problem with specific warrants.

Q67 Matt Warman: As an example, therefore, what do we not have access to that the security services would wish we had, and does the Bill plug that gap? I can see that the calendar is a very good one, but I am not sure whether, as Sir David says, it is covered by this. There is obviously some dispute between the experts in front of us.

Professor Jackson: It is not just a dispute between the experts. If you look at the proceedings of another Select Committee, the one that dealt with the bulk collection of data by GCHQ, they identified three types of data: one that was clearly metadata, one that was clearly content and a grey area. That is not reflected in the Bill as it stands.

Q68 Carol Monaghan: I was going to ask a bit more about the blurring of communications data with communications content. Do you feel that the Bill recognises the blurring of the lines between the two? Is there still some ambiguity surrounding them in the Bill?

Professor Omand: It is probably as close to precision as you are going to get. Where you are dealing with bulk data, you are talking about a Secretary of State's warrant. The Bill provides for different categories of Secretary of State warrant, then to be judicially reviewed by a senior judge. That already has the highest level of authorisation possible.

I think we are talking about cases where communications data—who called whom, when and how—can be obtained on the authority of, for example, a senior police officer who is not in the line of command of a particular investigation. The Bill provides for points of contact—SPoCs and so on—to do that. The question then is do you feel nervous that that kind of information can be obtained on the say-so of a senior officer, subject to the commissioner examining a proportion of cases and so on? That seems to me the only real issue that this definitional question brings up. It is about the level of authorisation.

Dr Wright: Could I jump in there? There is certainly some recognition of the grey area in the middle. Entity data and event data are pulled out, separating those two terms. Fundamentally, the problem I have with this issue is that the difference between content data and communications data is a proxy for how sensitive that data is. There is a fundamental philosophy in the Bill that communications data is less sensitive. That simply does not hold.

Fundamentally, we have these two different classes of access because we are saying, "This one is less sensitive and this one is more sensitive." To give a completely trivial example, if you were to watch a film via Netflix, the content of that communication is the stream of bits that are the pictures on the image, which are not sensitive at all. Within the context of the Bill, this would be access to Netflix, but when you choose to watch a film seems to me far more sensitive. It is not highly sensitive, but it is far more sensitive than simply the content of that Netflix film, which is seen by millions of people around the world. The

understanding that we do not have, and which is being hammered further into the axions of the Bill, is that communications data is not sensitive. That is a fundamental misunderstanding.

Professor Omand: I do not think that the authors of the Bill are saying that it is not sensitive. Clearly it is sensitive, but not as sensitive. There will be exceptions; you will always be able to find exceptions, but for most of the time it is a fact that the suspect's computer was communicating with the Netflix computer. In some circumstances, it could be a significant fact. Most of the time, it will not be. That is where the practical distinction lies. The alternative is to say that the higher threshold of the Secretary of State and the judicial review applies to every one of the half million accesses to communications data that take place annually at the moment. That is a proposition I would not want to entertain.

Q69 Carol Monaghan: The draft Bill currently states that communication data does not include the content of a communication, but Professor Anderson is saying that a calendar could be considered communications data. Therefore, the content would be subject—

Professor Anderson: Yes. A calendar says who met whom and when. That falls under the definition of communications data. What is more, related communications data includes communications data that is extracted by mechanical means from contact. Let me give you an example. If I send you an e-mail saying, "See you at the pub at 9 o'clock," and you are using a system like Google+, it will understand that and will remind you at a quarter to 9 that you are seeing Ross at the pub. That becomes communications data, even though it was in the body text of an email. The Snowden revelations show that these techniques are not used merely by Google—they are used by the NSA as well.

To follow up on my friend's comments earlier, the relative sensitivity of content and communications data is something that has come up again and again in this area over the past 20 years. When one speaks to operational police officers, they very often say that the communications data are the gold dust. If you have tapped somebody's phone or have put a room bug in their house, the sort of thing that you get is, "Fred, see you in the usual place in 20 minutes." Knowing who is calling whom tells you who is a member of a criminal conspiracy. The cell site location history of their mobile phone and the GPS location history, which is available, provide the real gold dust. Finally, bear in mind that the main privacy case in UK law is Campbell *v.* Mirror. Why? Because the *Daily Mirror* photographed Naomi Campbell leaving a branch of Narcotics Anonymous. A photograph taken on a public street is communications data. The High Court ruled that that was highly sensitive.

Professor Omand: From your earlier discussion on encryption, there is no doubt whatever that communications data—who called whom, where and how—is the gold dust. There is absolutely no disagreement about that. That is why the intelligence community and the police are so desperate to get the Bill passed.

Professor Jackson: In presenting the Bill, the Home Secretary stated that the data that would be made available would be the equivalent of an itemised phone bill. I do not think that the data we are talking about is the equivalent of an itemised phone bill. It has significantly more information content than an itemised phone bill gives.

Dr Wright: I want to hammer this point home more and more. The fundamental issue is that comparing it with telephony is ludicrous. In the modern world, particularly for younger people, a much closer analogy is with the real world. When did you go into your house? When did you leave your house? Which friend did you meet? What shop did you go into? What newspaper did you read? What book did you buy? If we were asking for bulk collection, retention and access to that kind of data in the real world, there would be uproar. Somehow, because this is the internet and it is slotted under "This is just telecommunications," the Bill has got to where it is.

Q70 Carol Monaghan: Do you feel that the language has to be clearer about what is meant by communications data?

Dr Wright: The conceptualisation has to be clearer. There is a fundamental misconceptualisation of what is going on with this kind of data.

Q71 Stella Creasy: There is an issue for us as a Technology Committee, because we are looking at the technology climate, but it does throw up the ethical questions. Sir David, I am very struck by your saying that we can never get a perfect world, but we can get a better technical response, can't we? That is at the heart of some of these questions, if it is capable of that—I accept Professor Anderson's analogy. After all, if I send an email to Outlook about a diary meeting, then whoever it is sent to, it will be a diary update. All you would get is the contact data, but knowing that I am sending an Outlook update, you know I have a meeting with that person, so you can build a picture. It is entirely possible to do that. Some of these are questions about transparency. While all of us recognise the challenges around what Edward Snowden did, the fact is that there is now a debate about what is the right information, because we recognise that people are using these technologies. The other side is the technological capacity. What I am struggling with, and what is coming out very clearly from what you are saying, is whether the British public understand fully what is currently capable of being grabbed in this way and, therefore, where that might go. Then when we have these debates we can have them with transparency about what is capable. When you talk about worst case, there are also the everyday cases, so, when we go to robot cars, it will not just be the foreign dignitary's car that you might be able to trace, but my car and your car. Therefore, we need to have a conversation as a society about how that data is handled.

Professor Omand: I am very comfortable with what you have said, except that I would hope the Committee sees the part of the picture that has not been mentioned at all, which is why this Bill is necessary: in other words, what the harms are. That, too, has a technical component, which is of some interest. It has already been touched on with the spread of end-to-end encryption. If you want a society in which the law is upheld, where criminals are brought to justice and terrorists are tracked down, then you cannot have a society in which you do not have some of these powers. It is a question of where you draw the line.

Q72 Stella Creasy: I understand that, but as somebody who was not able to make progress in tracking somebody who was harassing me online, because they were using the Tor network, the flipside of this is about our understanding of the technological capacities and limitations. Do you think there are elements in the technological aspects of this Bill, of the internet, and how it is progressing, that the public are unaware of, that maybe the security

services are not aware of, and therefore that limits what the Bill can take us forward and do? If so, how would you address them? I would like to ask all three witnesses.

Professor Omand: This Bill only takes us a certain way forward, so there is compromise to be arrived at between the needs of keeping us safe and secure and the needs that people feel for a reasonable level of privacy, unless you are going to take an absolutist position one way or the other. As a witness I want to be somewhere neatly in the middle on that. You mentioned Tor. The problem with Tor is not necessarily the anonymity it provides its users. Facebook is now on Tor, so that it can provide an additional level of security for its users. The *New York Times* has a site on Tor, so that if you are a whistleblower you can provide information in confidence. The real problem with Tor is that it also hides the identity of the people running the websites on hidden services, the criminal websites, where you go to buy guns, drugs or malware. It is neither right nor wrong. Encryption is just a technology. It can be used for good and it can be used for evil.

Q73 Stella Creasy: That was not quite my question. I would be interested to hear from the other members. I would imagine that in a free society we all think whistleblowing is quite an important thing to be able to do.

Professor Omand: Yes, absolutely.

Q74 Stella Creasy: Are there other technical ways in which we could help the security services and the police—because this expands from things that the security services are doing through to the police—that would work better with technology as it is and as it is to come? One of the elements is the disjuncture between the technological capacity of, perhaps, our public services and what they are seeking to do. I do not accept that this is an either/or, this is the worst case, this is it and nothing else. Are there technical improvements that could be made? Professor Anderson is itching to come in.

Professor Omand: I would have gone slightly further than just the internet connection records. As you have just heard, it is a burden on the company to separate that part, and having a full web log would be rather more useful. I can perfectly well see why that is not thought to be saleable at the moment, and I would not push the case, but it is just an illustration that there are things that can be done if society wills it.

Professor Anderson: The main limitation is that we live in a globalised world, and the great majority of the services of interest are not UK services. Most are American. Some are Korean and so on. Although there are technical things that could be done to improve things, such as training the police better, getting them to specialise more and so on, the fundamental problem is that when you try to bully foreign companies they react by introducing measures such as encryption. Many of these problems are of the making of Governments themselves. Let me give you an example. The biggest problem facing service companies like Google is that you get a court order from a family court in India saying, "Hand over all the Gmail of this person in Canada and keep quiet about it for ever." If you are running Google, how do you simultaneously employ engineers in India and be honest with your customers in Canada? The answer, as chosen by more and more firms such as Apple, WhatsApp and so on, is that you encrypt the stuff end to end so that

you can say to the court, "Sorry, guv'nor, I don't have it." The technology and the policy are inextricably intertwined, and the background that every legislature has difficulty grappling with is the fact that it is a globalised world, and the way forward is probably through treaties rather than through technology. Something like the cybercrime treaty, but a cyber-evidence treaty instead, would probably do far, far more good than many of the things that we see in the Bill, but that is hard. A Bill is easier to get through if you want a result in a single Parliament.

Dr Wright: In the previous discussion, you raised how we break encryption or how we break through Tor. My reaction, on issues such as Tor, is that it would certainly not be with the bulk retention of data. There are traditional methods to investigate the activities of individuals, and they involve targeted means. I believe that, in general, there is an increasing reliance on this gold dust, this magic bullet, of global content data through which, almost by definition, it is very difficult to detect crime. The purpose, as I understand it, of bulk retention of data, is that when you become interested in an individual you suddenly have a time machine that can take you back 12 months to watch what they did. I completely understand the desire for that kind of information. I am much more sanguine about starting to watch somebody when you suspect what they are doing; you can start to investigate them and their social networks. I certainly support provisions to achieve that within reason, and within the constraints of things like end-to-end encryption, which ultimately is what I would call a hard problem. There is a lot of focus on organisations, such as telecommunication providers, but with a lot of the software that is increasingly coming out now a user can download and install an open-source piece of software for free on their phone or computer that is not linked to an organisation or a company. I had a student last year who was looking at the use of encryption software by jihadi groups. They have their own home-grown encryption software. They are not going to mandate that al-Qaeda install a back door or provide your access to communications data. These are people using their own computers. There has to be much more focus on a more traditional approach to investigating individuals.

Professor Jackson: My view of the Bill is that it is doing something which is a blanket approach by taking everybody's data for possibly very little gain; only a very small percentage of that data will become useful. In the way the Bill is phrased at the moment, although I perceive it as a reduction of privacy, it is not a big enough reduction to make a big change. In some ways, it is edging us down a route that goes to less personal privacy without giving us a whole load of gain. As we have just said, because of the technical aspects, there are ways of subverting what the Bill is doing, which those who are liable to be involved in terrorist activities, who are liable to be the people committing crime, will certainly make use of. Because there is now a Bill, they will be aware that they should be making use of it. The gain is not going to be very great but the cost, which we have talked about, in terms of all this data that has to be stored, will be quite high. Also the erosion of privacy, which we have begun, may effectively be the first part of a descent into an eventual solution where, okay, we have a situation where we are more able to clamp down on terrorism but we have thrown away a huge amount of privacy rights.

Q75 Valerie Vaz: Touching on what you have all said and picking up from you, Professor Jackson, could each of the panel say what you know about the extent of current bulk

communications, interception and data access? I don't normally do two-headed questions, but would you describe it as mass surveillance?

Professor Anderson: Absolutely. This is something that had been known to insiders for some years, as Sir David made clear, but the Snowden revelations brought home that, for example, all the data en route from one Google data centre to another was being hoovered up, and all your Gmails, all your Google calendar and so on were vanishing into the machine. If that isn't mass surveillance, somebody is redefining language.

Professor Omand: I would flatly disagree with what you have just heard. In terms of the United Kingdom—we are talking about the United Kingdom and the effect of UK legislation—bulk access to internet communication is not the same as mass surveillance. These are different concepts. The senior judge, the interception of communications commissioner, in April 2014, in March 2015 the court, the IPT in December 2014, the Intelligence and Security Committee, David Anderson QC, and the panel I was on, the independent panel set up by Nick Clegg, all looked at this and all came to a unanimous conclusion that it is not mass surveillance. Mass surveillance is the persistent observation of all or a large part of the population. That does not take place in the United Kingdom.

Professor Jackson: The evidence for this is the report of the committee that looked at GCHQ's bulk data collection. It was clear that there is collection of bulk data, but if we accept the evidence taken by that committee, we have to say that only a very small percentage of that data is looked at and examined, and we have to do that. The reason given for that, if you read the report, is partly that there is, as yet, not the technical capability. Although we are making inroads into big data research and processing huge amounts of data, there is, as yet, not the technical capability in GCHQ—this was given as evidence—that that whole set of information can be processed. Clearly, we have been talking about technological evolution, and it is a major research area at the moment to be able to process data automatically, make conclusions and find information from processing huge amounts of data. In some ways, the supermarkets are already ahead of us with their reward cards and so on. In the future, the very fact that that data has been collected may open it up to mass surveillance in new ways. Again, there are some safeguards in the Bill about that. Going through to that mass surveillance, there are more safeguards than we previously had. One has to say that it is more possible to make use of that data looking forward than is happening at the moment or has happened in the past.

Dr Wright: I broadly agree with that, so I won't play semantic games, which is always fun. Ultimately, this comes down to surveillance and interception. Again, it falls within some of the language in the Bill. There is a stated view that something is only surveillance when it involves a person reading or intercepting some data, or as a result of some analysis. That is a fundamental philosophical point. I would argue that, when you have the gathering of this amount of data, you are certainly falling under what is beginning to touch on what people would understand as surveillance. You may be able to make the argument, "This is not surveillance because we never looked at it." Increasingly, as Professor Jackson just said, we are getting the capability to manage big data and to run analytics on big data, which means you can do a huge amount with data in terms of coming up with trends and patterns of activity about individuals and groups, before a human ever gets involved in the loop. I can imagine situations in which a human is never involved in the loop.

If I can expand on that ever so slightly in terms of the public perception of this kind of work, a survey of 1,200 people was done about the Snowden revelations, or provisions like that, in terms of the surveillance of Government; 78% of the people involved felt that they would need to be more careful about their speech and online searches in light of the Snowden revelations. There was also an empirical study of the number of views on a number of sensitive topics on Wikipedia. In May 2013 there were just under 3 million views combined of those searches. In June 2013, after the Snowden revelations, there was a sudden drop of 20% in the number of people looking at those pages. People are scared when they learn about this. People stop accessing perfectly legal, legitimate and normal information because they are scared of those programs. That turns into a decreasing trend. The chilling effects that were mentioned earlier are real and empirically backed.

Q76 Valerie Vaz: I want to pick up the point I made earlier about handling arrangements for bulk personal datasets. Obviously, I could ask you all why, and you could give me a reason. Why do you think that it was passed outside the Bill? Why is it not part of the Bill, and why has it not been defined in the Bill, because it can extend to our medical records, can't it?

Professor Anderson: There are significant public sensitivities about medical records, which are purely of interest to some agencies, if they are permitted to get their hands on them, and normally would fall under other regulations and other departments. Let me give you another example—your bank statements. How many Government Departments do you want to have access to your bank statements? Do you want a policeman to be able to access them as being, in some sense, less sensitive data? For what purposes would you want, for example, credit reference agency files to be useable? To what extent would you want an investigation to take place by running automated programs over all the bank accounts of everybody in the UK? For example, looking at missing VAT might be the sort of thing that people would start off with, and then—who knows—within five years it would be missing expense claims or duplicated expense claims. Once you start giving automated access to vast amounts of data like that, where are the checks and balances? How do you stop it going from something that most people would agree with, such as looking through foreign bank transfers to look for criminal and terrorist funding support, to something that voters would find personal and oppressive?

Q77 Valerie Vaz: But personal data is not part of the Bill, though, is it?

***Professor Anderson*: Yes.**

Valerie Vaz: It's already come into force, and it's not even defined.

Professor Omand: Clauses 151, 152, 153 and 154 in the Bill all set out processes.

Q78 Valerie Vaz: Why was it brought into effect before the Bill comes into effect?

Professor Omand: Because the Intelligence and Security Committee, no doubt rightly, talked about this, and therefore the Government—

Q79 Valerie Vaz: But it is not going to be scrutinised, is it? The whole point of having a Joint Committee is to scrutinise those elements, and it is not going to be scrutinised. It has already come into force.

Professor Omand: It is going to be scrutinised. It is in the Bill.

Q80 Valerie Vaz: But it has come into force already, so it is happening now, isn't it?

Professor Omand: The existence of bulk access for the security service, say, to the vehicle driving licence database, which seems to me a perfectly reasonable thing for them to want to have pretty quick access to for all sorts of reasons—

Valerie Vaz: Professor Jackson?

***Professor Omand*:** May I finish? The Bill has a whole section on bulk personal datasets. A warrant is going to be required from the Secretary of State, scrutinised by the judge, on the purposes for the dataset is needed, and there are time-expiry rules. You can go through each of those, and I hope the Committee and the Joint Committee will look at that, but we can scare ourselves witless about possible abuses. That is why it is so important that this Bill has tightened up oversight and judicial. When we took evidence from a lot of internet companies, particularly the American ones, as part of the RUSI—the Deputy Prime Minister's—review, most of them said in private, "Look, we want to help. We do want to be able to provide this information, but we would like to see Parliament legislate. We would like to see a warrant and we'd like to see a judge's fingerprints on it. Then we will be able to deal with our overseas customers and say 'It's all perfectly above board'."

Q81 Valerie Vaz: Professor Omand, I am sure you have read, as I did when I was in the civil service, "The Judge Over Your Shoulder," written by Roland Phillips. I am sure you know it. You will know that this is not a judge looking behind what the Home Secretary is doing. The judge is just looking at process. That is what judicial review is. They are not looking at reasons.

Professor Omand: No, no. That is quite wrong. I am sorry, it is a point of fact.

Q82 Chair: This is not the Home Affairs Select Committee, although I have fond memories of it. We are talking about the technical issues.

Valerie Vaz: But it is about access to data, isn't it?

Professor Omand: Judicial review that involves human rights is not just process. I am sorry that is wrong.

Q83 Valerie Vaz: Professor Jackson?

Professor Jackson: I think you were asking a question about bulk data collection.

Q84 Valerie Vaz: I am partly asking why it was not part of the Bill.

Professor Jackson: The answer is that it is covered in the Bill, but it is legal because it has been legal from—I am not a legal expert on this one—an earlier Telecommunications Bill which made it legal for GCHQ to collect bulk data, and that was confirmed by the RUSI panel that Professor Omand sat on.

Dr Wright: I do not have a huge amount to add. It ties into the entire argument that the Bill is just extending existing powers—a fact that I dispute—but that is probably the reason why it is minimal, if it is there at all.

Q85 Chris Green: Dr Wright, do you have any concerns about access to data on services hosted overseas, such as cloud computing, Gmail and so on?

Dr Wright: With respect to that, it is probably most closely tied to the concerns that were raised by the previous panel about the willingness of companies abroad to do business in the United Kingdom. One of the major concerns is that we are creating an environment where companies will be pushed to avoid the United Kingdom because they are being put into a situation where they have to comply with what they would consider unreasonable demands. Beyond the concerns raised there, no.

Professor Jackson: The concern I would have is that it is part of the weakness of the Bill that there may be overseas countries that are willing to collaborate, and there will certainly be overseas countries that do not collaborate. Therefore, that will push people who are seeking to subvert what the Bill is trying to do to use overseas providers as a way of making sure that they are able to carry out whatever terrorist activities they wish to carry out without being identified by our own security services.

Q86 Chris Green: This goes on to what was discussed earlier by Professor Anderson about treaties being so important. If we develop the Bill here, we are going to have to have treaties with countries overseas, to work with them to get some kind of consistent approach.

Dr Wright: Which may turn out to be difficult. As we have seen in the US, the direction of travel may be in an opposite direction from the way the UK Government are going with this Bill. It is generally seen that the Bill is rather more stringent than any other Government seem to wish to pursue. In that case, we may be putting ourselves in a position where we are unable to collaborate with other Governments because we have produced a Bill which has stricter requirements than other Governments have.

Professor Anderson: This is really key if we are going to get a cyber-evidence convention, which is what we will probably end up with in the long run, in 10 to 20 years' time, because other countries, such as north America and in western Europe, have a different approach to things like wire taps from us. In a great majority of those countries, wire taps can be used in evidence and are used in evidence. They are also authorised by a judicial warrant rather than a warrant from a Secretary of State. A future cyber-evidence convention will probably say that country A can get stuff, content and communications data, from country B provided, first, that an independent person, such as a judge, has accepted that there is probable cause, reasonable suspicion or whatever, according to local

law; secondly, that there is transparency, which means that the people whose stuff is got at get told eventually, when they are charged or when the investigation is dropped, or after seven years otherwise; and, thirdly, that there is respect for jurisdiction. Those are the three pillars on which a cyber-evidence convention will have to be built. They are against the GCHQ culture and they are against the provisions, the spirit and the general grain of the Bill. My own feeling is that we will be back here in 10 or 15 years doing it again, so that we can fall into line with the ways that America, Europe and other OECD countries will be behaving by then.

Q87 Victoria Borwick: How can the competing demands for gaining access to encrypted communications and protecting such communications be reconciled? We touched on this slightly with the earlier panel.

Professor Omand: The starting point has to be national policy, which is, "It's the economy, stupid." We depend on the internet. Therefore, security of the internet is the No. 1 priority. If there is any doubt over admitting to some flaw which has been found, or over retaining it for computer interference, it gets disclosed. It seems to me that the policy on this is extremely clear. Indeed, both this Government and the previous Government made it very clear in their cyber-strategies that you need strong encryption. We need to be able to rely on the internet. Criminals don't normally conduct their crime by breaking the encryption anyway, but do you want deliberately to remove what I would describe as the right to seek on the part of the police and the intelligence agencies—to try to find out if they can get a lead on some terrorist group, criminal group or paedophile network? We should be encouraging them to try, but there is no guarantee. I am certainly not advocating back doors being mandated, things which would weaken the integrity of the internet; there is a lot of nonsense talked about all of that. But they have to try, and some of the Bill would enable one or two tricks of the trade to be applied. Computer interference is one of those, which might give them a chance to get across some of the most dangerous people who are out there. I don't think you can ask for more than that.

Q88 Victoria Borwick: One of the queries that my colleague raised earlier was whether encryption has got so complex that it prevents the law on surveillance and those who need to be—

Professor Omand: It clearly does.

Professor Anderson: As a general proposition, the encryption algorithms used today cannot be broken if they are properly implemented. There is evidence that certain agencies can attack algorithms with certain reduced key lengths but, in general, encryption does not get broken. It is end systems that get broken or else the keys get stolen. The right way to get round encryption is targeted equipment interference, and that is hack the laptop, the phone, the car, the Barbie doll or whatever of the gang boss you are going after, so that you get access to the microphones, to the cameras and to the stored data. The wrong way to do it is bulk equipment interference. It is tempting, if you are an intelligence agency, to say, "We don't like North Korea, so we want to bug all the phones in North Korea, so we will put malware in all the phones in South Korea so that those that find their way across the border will have bugs in them." This may be rational if you are running a hostile intelligence agency, but in a world in which we all depend on each other it is bad stuff.

And it is seriously bad stuff when we start doing it to fellow members of the European Union, because it will get us into all sorts of trouble with the two European courts, not to mention the European Parliament.

Q89 Chair: Does anyone else wish to comment? I am conscious of time.

Professor Jackson: Encryption is vital for commerce to happen on the internet. There is a theoretical debate that it could all fall apart with one scientific discovery. If that happens, we would have a serious problem with the economy.

Q90 Matt Warman: I would like to make one quick point. One of the things Professor Anderson said was "Where are the checks and balances?" and Dr Wright talked about the so-called chilling effect of what people search for. Ultimately, the checks and balances are in Parliament. Whatever technical discussions we are having, is it ultimately down to us in Parliament to make the case that we are technologically competent to draw up some sort of legislation that we in a civilised society are comfortable with? That is not to do with technology at all. Is that fair?

Professor Omand: I agree with that. I am sure you and the Clerks have access to a lot of expertise, but you can also, in this Bill, make it clear that the judges who are going to oversee this need a lot of technical expertise at their fingertips—that is those who go in and inspect how the algorithms are being used. There is quite a lot of work to be done to raise the general level of oversight of competence. The Intelligence and Security Committee will also need technical expertise.

Professor Anderson: It is not just the experts. It is the motivation. It is what they are trying to stop and who pays them. One of my concerns about this Bill is that the Technical Advisory Board will have representatives of the police and intelligence agencies on the one hand, and of the telecom service providers on the other, but it is not going to have representatives from anybody else. It is not going to have representatives from civil society, NGOs, academia, the software industry and the many firms that are reliant on the internet and its trustworthiness for their business models, ranging from computer gaming companies to banks. In other words, the technical advice that will be available to the Home Secretary, and as part of the oversight process in the Bill, is fundamentally skewed towards only two of the many stakeholders who depend on the internet for their livelihood and their freedom.

Chair: Thank you very much. Unsurprisingly, that was one of the more heated panels we have had before the Committee so far. In closing, I do not think there is anyone on this Committee or in this House who is losing sight of the purpose of the Bill—that it is there in order to provide law enforcement and intelligence agencies with the powers that they need in order to fight crime in a digital age. The concerns that we have heard today about proportionality and clarity need to be properly scrutinised. There are questions about ensuring that the Bill delivers its intended aims without weakening encryption or exposing large volumes of personal data to security risks, and it is right that that should be properly scrutinised in this Committee and in others in the House.

Thank you for the help that you have given us today. If we have further questions, we will follow up. I hope that you will be happy to help us in our endeavour to translate the technology into plain English for colleagues. Thank you very much.