HOUSES OF PARLIAMENT

Joint Committee on the Draft Investigatory Powers Bill

Oral evidence: Draft Investigatory Powers Bill, HC 651

Monday 7 December 2015

Watch the meeting

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Bishop of Chester, Lord Henley, Lord Strasburger

Questions 76-100

Witnesses: Professor Ross Anderson, Professor of Security Engineering, University of Cambridge, **Dr Paul Bernal**, Lecturer in Information Technology, Intellectual Property and Media Law, School of Law, University of East Anglia, **Professor Sir David Omand GCB**, Visiting Professor, Department of War Studies, King's College London, and **Professor Mark Ryan**, Professor of Computer Security, School of Computer Science, University of Birmingham

Q76 The Chairman: We extend a very warm welcome to our four guests this afternoon. We are very grateful to all of you for coming along on what is a hugely significant Bill that is going through Parliament—the Prime Minister called it the most important of this Session. Thank you very much indeed. As you probably know, the procedure is that I will kick off with a question or two, and then my colleagues will in turn ask you various questions on different aspects of the Bill that I think you find very interesting. If, when I ask a question of an individual, he wants to preface his remarks with a short statement, that is entirely up to him. I turn first to Dr Bernal. After you have answered, colleagues will be able to come in. What are your views on the draft Bill? Does it deliver the transparency on investigatory powers that you have particularly called for?

> ***Dr Paul Bernal:*** Perhaps the best way to put it is that it goes part of the way. As far as I am concerned, it is good to see everything in one place, or almost everything—some bits are clearly missing—but for proper transparency we do not need just the Bill; we need the process to work properly as well. I would have said in my introductory remarks, had I made any, that the timetable makes it very difficult to get as much scrutiny as we would like; we have been called here very rapidly, and you have only a few weeks to do this. For transparency to work properly we have to have the chance and time to put our analysis into action. It is a bit difficult to do that.

One other thing I would say about transparency is that certain terms are used and expressed in a way that is not as clear as it could be. There are terms like "bulk powers" when we do not really know how bulky "bulk" is, if you see what I mean. For things like Internet connection records, it has taken some time, and we are still only part of the way there, to tease out what it really means. From that perspective, it is good to have it all in one place, but the process needs to be stronger. We need to make sure there is enough time to do it, and I am not sure you have as much of it in this Committee as you would like—perhaps later on there will be time—and we have to tease out some of the terms more accurately.

There is one other aspect. Some of the things in the Bill will become dependent on codes of practice and similar things that go with it. For transparency's sake, so that we understand what is going on, those codes of practice need to be put in a form that we can all see prior to the final passage of the Bill.

Q77 The Chairman: You have touched on the second question I was going to ask, so I will raise it now. You mentioned the codes of practice, which are hugely important in all this. What do you think the legal status of those codes might be?

Dr Paul Bernal: The legal status of the codes depends a little on how the final Bill turns out. From our perspective as legal academics, the key thing about codes of practice is not so much their legal status, which, depending on how it is set out, will be clear, but the extent to which they are also subject to the level of scrutiny and attention that the Bill itself is. It is easier to pass a code of practice through a small statutory instrument than to pass a whole Bill with full-scale scrutiny. We want to make sure that the codes of practice, which can be the critical part, get the same degree of scrutiny and attention both from people like us and from people like you.

The Chairman: With regard to the timetable, of course the issue that affects both this Committee and Parliament is, as you know, the sunset clause in the current legislation. Parliament has now laid down the amount of time we have. We certainly ensured that we gave ourselves extra and longer sessions, including in and around Christmas, and I am quite convinced that both Houses of Parliament will give it very thorough investigation, as indeed they should, but the point has been made. Does anybody else wish to speak on those issues?

Professor Sir David Omand: If I may make two remarks, the first is to stress the importance, in my opinion, of the Bill as the culmination of 500 years of history. It has taken 500 years to put the secret surveillance activities of the state under the rule of law. For centuries we had the royal prerogative being used in secret. Parliament passed the device of the secret vote but asked no questions. We had executive regulation in the last century, and for the past couple of decades we have had a patchwork of provisions in legislation, so all that secret activity was lawful but not understood. This Bill now places it under the rule of law; it will be comprehensible to the citizen. I cannot overestimate the importance of the Bill.

The second point is to agree strongly that it is in the codes of practice that the public will find it easiest to understand what is going on, rather than in the technicality of the Bill itself, so the codes are very important. Schedule 6 to the Bill sets out very clearly what the

status of those codes will be. They will have to be presented to Parliament, along with the enabling statutory instrument.

The Chairman: Professor Anderson or Professor Ryan, are there any comments you would like to make at this stage before we move to other questions?

Professor Ross Anderson: I believe you will be asking me in due course about Internet connection records.

The Chairman: We will.

Professor Ross Anderson: It would be great if, in addition to having codes of practice, we had very much greater clarity on definitions. I will discuss Internet connection records, but there are other things that are not really defined at all, from the great concept of national security down to some rather technical things. I hope that clarification comes out during the Bill's passage.

The Chairman: You think such definitions should be on the face of the Bill.

Professor Ross Anderson: Yes.

The Chairman: Professor Ryan, are there any initial comments you would like to make to the Committee?

Professor Mark Ryan: Just on questions 1 and 2?

The Chairman: At this stage, yes, because there will be other more detailed questions, some of which will probably be directed to you personally as well, but at the beginning of the session would you like to make any general comments?

Professor Mark Ryan: The comment I would like to make about transparency is that this seems to be such an important area that the kind of oversight proposed is not enough. One would need more quantification of the sort of surveillance that takes place. Of course, I am aware that surveillance has to be done in secret, but I believe that the quantities of surveillance and the nature of surveillance can be disclosed to people without compromising the secrets of the surveillance activity. That seems to go more towards transparency and is much stronger than mere oversight, so I believe there should be more of that.

Q78 Dr Andrew Murrison: You have covered a huge amount of ground in about seven minutes. You hit the nail on the head in terms of definitions and the need to ensure that codes of practice and statutory instruments are sufficiently transparent and that scrutiny is of the utmost. I am interested to know how you think scrutiny and transparency can be improved other than through the normal process of laying statutory instruments before the House, because I sense from what you said that you feel that the Bill, which talks about SIs and codes of practice, is not sufficient in that respect.

Dr Paul Bernal: I would not say exactly that it is not sufficient. What I am interested in is getting as much scrutiny as we can. In order that we can understand the Bill we need to have the codes of practice at the same time, at least in draft form, so that they can be examined; frankly, to understand some of the powers in the Bill without a code of practice is very difficult, particularly on things like bulk powers and Internet connection records. We will talk a lot about Internet connection records later, but they are defined in such a way that it is unclear on the face of the Bill exactly what they will mean in practice.
Historically, not as much attention is paid to statutory instruments by the House. You do not spend as much time passing them as you do Bills; you do not have Committees scrutinising each of the statutory instruments at the same level of detail.

Dr Andrew Murrison: But it is worse than that, is it not? This is a very rapidly moving field, so you cannot reasonably lay all the codes of practice and anticipate all the SIs at this time, since 12 months down the line there may be yet more to come.

Dr Paul Bernal: Yes, and that is a fundamental problem with any kind of Bill in this area. I do not know whether there would be a mechanism to produce better scrutiny of the codes of practice, but attention should be drawn to the fact that this will be important as it continues. It needs constant attention, not just at the moment we pass the Bill.

The problem with the Regulation of Investigatory Powers Act was that, although it got a lot of attention at the time, the things that gradually built up to create the confusion—chaos is not quite fair—for people about the overall regime, and which stimulated the need for this Bill, were not sufficiently attended to over the years as things happened. We need to make sure that does not happen this time around.

Dr Andrew Murrison: Do you think a sunset clause would help? We are replacing one sunset clause with another. Is that inevitably where we are going to be led?

Dr Paul Bernal: Frankly, in this area you need sunset clauses in almost everything, because the technology moves and the behaviour of people changes. The overall situation changes. You need to be able to review these things on a regular basis, and a sunset clause is one of the best ways to ensure that happens.

Professor Ross Anderson: Last time around how we dealt with this was that, in the run-up to the passage of the Regulation of Investigatory Powers Bill through Parliament, a number of NGOs organised a series of conferences called Scrambling for Safety, and afterwards various statutory instruments were laid before the House. We are proposing to do the same again. The first Scrambling for Safety workshop is to be held at King's College London on 7 January from 1 pm to 5 pm, and all members are of course very cordially invited. We anticipate that it will be the first of a series that will enable engineers, lawyers, policymakers and others to dig into the meat of what is going on, exchange views and push the thing forward.

Q79 Suella Fernandes: Based on your expertise, would you set out briefly the nature and extent of the problem or threat we are facing when it comes to the use of this technology?

Professor Ross Anderson: The problem with the use of surveillance technology is that, if it is used in ways that do not have public support, it undermines the relationship of trust between citizens and the police, which has been the basis of policing in Britain for many years. Sudden revelations like Snowden are extraordinarily damaging because they show that the Government have been up to no good. Even though the Government may come up with complicated arguments about why bulk equipment interference was all right under Section 5 of ISA and so on, it is not the way to do things. There was a hearing in the Investigatory Powers Tribunal last week on that very issue.

There are other issues. The first is national leadership. If we go down the same route as China, Russia, Kazakhstan and Turkmenistan, rather than the route countries such as America and Germany have gone down, there is a risk that waverers, such as Brazil and India, will be tempted to follow in our wake. That could lead to a fragmented IInternet, with extraordinarily severe damage for jobs, prosperity, international stability and, ultimately, the capability of GCHQ to do its mission, because if you end up with the IInternet being partitioned into a number of walled gardens, like the Chinese or Iranian ones, they will be very much less accessible to the intelligence agencies.

In addition, if the powers are abused, or seen as capable of being abused, there could be exceptionally serious damage to British industry. If people overseas come to the conclusion that, if they buy a security product from a British firm, it may have a GCHQ-mandated back door, they will not buy it; they will buy from a German firm instead. This is where the rubber hits the road when it comes to overreach in demanding surveillance powers.

Professor Sir David Omand: On the other hand, my advice to the Committee would be that this Bill contains the basis of the gold standard for Europe. This is how you get both security and privacy in respect of freedom of speech. The interplay of checks and balances and oversight regimes means that none of what Professor Anderson has described needs to happen. Of course, with a malign Government and agencies that flouted the law it would be possible to have abuses. I do not believe that either is likely, and certainly the provisions in the Bill allow this House to maintain very strict control of the Executive in its use of these powers.

Professor Ross Anderson: With the greatest respect, the reaction of America and Britain to the Snowden revelations has been somewhat different. In America people have rowed back in all branches of government. For example, President Obama has, simply by executive order, commanded the NSA to minimise the personal information of unaffected foreign nationals, like us. The legal branch has seen to it that, for example, national security letters, which used to be secret for ever, are now disclosed after three years, and Congress failed to renew provisions for the retention of American citizens' communications data. All branches of government have pushed back and sent a solid signal to the world that America cares about privacy and the proper regulation of its law enforcement and intelligence services. If the reaction from Britain is different, even if powers are not abused, it still sends a signal to the Brazils, Indias and, may I say it, the Kazakhstans. We do not really want that.

Q80 Bishop of Chester: A sunset clause is the nuclear option of legislation, but reading the Bill I am wondering how there is a process of inbuilt review, because the scene is changing so fast. There is a technical supervisory board bringing together stakeholders and so forth. Should there be an inbuilt power to renew the provision? That has been in some previous terrorist legislation. There has not been a formal sunset clause, but there has been a renewal motion. That would force Parliament to review what is happening, because for the legislation to continue there would have to be a renewal notice.

Professor Sir David Omand: Of course, it is Parliament's prerogative to put in such a provision. My experience in the public sector is that it should be done very sparingly, because it may turn out that at precisely the moment you have to legislate afresh, as with DRIPA, Parliament may not actually want to legislate afresh. One concern I had was whether the definitions in the Bill were sufficiently robust to deal with technical change. Having studied them, I am as confident as I can be that they avoid hostages to fortune, so your House will not discover in a couple of years' time that a different Bill is needed because the technology has moved on, but that will need to be examined by detailed scrutiny.

Q81 Shabana Mahmood: My first question is to Professor Anderson and then his colleagues. We have two competing narratives of the Bill: one that these are significant new powers and major changes, and the other that it is just codifying current provisions and bringing them more obviously and explicitly within the rule of law, as Sir David suggested. Professor Anderson, what is your view as to which of those narratives is more accurate?

Professor Ross Anderson: The Bill has been marketed as bringing in only one new power, namely IInternet connection records, but it does many other things as well. For example, when the Regulation of Investigatory Powers Bill passed through this House and became an Act, one of the things we lobbied for and secured was the provision that if the agencies wished to command somebody to decrypt something, or hand over a cryptographic key, there should be special safeguards. The City of London did not want a rogue superintendent, perhaps in the pay of a criminal gang, to approach a 24 year-old assistant shift supervisor at a bank's data centre somewhere in east London and command him to hand over the bank's master signing key. Therefore, the provision was made that the production of a cryptographic key had to be demanded by a Chief Constable in writing and the letter had to be presented to a main board director of the bank. There are many provisions like that which appear to be swept away by this new legislation. Parliament must realise that the arguments are just as strong today as they were then; otherwise, how are you going to persuade international banks that London is a good place to do business? Some banks already had issues last time around.

My second comment is that a number of things that were previously done secretly were made public only in the run-up to this Bill, which enables the Bill team to say, "This is old stuff. We knew about it already". I refer members to the Investigatory Powers Tribunal hearing and the long arguments therein about whether an ISA Section 5 warrant could be used for bulk interception or only targeted interception. There are many technical aspects like that.

Thirdly, although the IInternet connection record is ostensibly the new thing in the Bill, it actually gives very much greater powers than have been advertised; rather than just

helping IP address resolution, it enables a policeman to say, for example, "We have these two bad people. Show us all the websites they both visited last month, and tell us the names and addresses of everybody else in the world who visited the same addresses". That is an extraordinarily powerful capability. It is the sort of thing that IInternet service companies use to fight spammers, phishermen, click fraudsters and so on. Those of us who have worked in that field know how powerful it is and tend to be of the view that it should be classified along with intercept. If we are to have a special higher burden for intercept warrants, that higher burden should apply also to complex queries that are made on traffic data.

Shabana Mahmood: Have you done any analysis of powers advertised one way but which, as you suggest, lead to, say, five extra things? Have you made some sort of qualitative analysis to back up the examples you are helpfully giving us?

Professor Ross Anderson: The qualitative analysis basically comes from experience working at Google on sabbatical four years ago with the click fraud team. Knowing that such inquiries are extremely powerful, and talking to colleagues at Yahoo and Facebook recently, there is general concern that, if you allow people to make complex queries like that, it is up at the level of a box of fancy tricks; it is not the sort of stuff you want to let an ordinary policeman do without supervision, because it can be used to do some very bad things.

Professor Sir David Omand: The Bill does not provide for ordinary policemen just to request that. There is a mechanism for a single point of contact and independent agreement before data can be acquired. I do not recognise either of the extreme cases Professor Anderson puts forward, but no doubt the Committee will need to investigate that further.

Dr Paul Bernal: If I may add something in response to that, there is something missing in the idea that these are either new powers or old powers. People's behaviour has changed fundamentally. The Internet, which was a medium used for communications—in the old-style idea of communications—is now used for almost everything else: shopping, dating, research and that kind of thing. The same power applied in a different situation gives a significantly higher level of intrusion than we have ever seen before. It is not like listening to phone calls, reading emails or things like that; it is like following people down the street while they shop, looking at the books they take out of the library and things like that. Without even changing the law, you are significantly changing and increasing the level of intrusion. It has lots of different implications, not just in terms of the balance of privacy and things like that but all the other rights we normally think of. Our expectations of privacy are different from those we had in the past. In a way, it comes down to the idea of how the law is going to change and how we need to take things into account. We need to take into account not only developments in technology but the way people's behaviour changes in relation to that technology; for me, in effect, that is the biggest increase in power. It is not that there is a new power built into the Bill, but because we use communications so much more extensively it is a much more intrusive thing to do any kind of Internet surveillance.

Professor Sir David Omand: That is why the Bill defines event data, Clause 193, in a conservative way, not taking modern metadata but imposing on the rather fuzzy reality

some precise definitions, to minimise—it cannot be avoided completely—the kind of case Dr Bernal referred to. Inevitably, if you impose strict definitions on fuzzy reality, you will occasionally get hard cases. Those will exist in this world. As we know, the difference between dangerous driving and driving without due care and attention means that sometimes cases fall on the wrong side of the line, but the old adage that you do not make law by hard cases still applies. I commend to the Committee the way that the Bill has not expanded the definitions of communication data in defining event data.

Q82 Shabana Mahmood: That is helpful. You touched briefly in your previous answers on my final question, which is about future-proofing the Bill to take account of the pace of behavioural and technological change. We had evidence from officials from the OSCT. They were very bullish and confident that the changes in relation to Internet connection records in particular meant that it was sufficiently future-proofed. Could we have your comments on that?

Professor Ross Anderson: I have two main comments. The first is from the viewpoint of the long term—20 years out. We are simply asking the wrong question. The right question is: what does the police service look like in a modern technological society? Is it completely centralised? Does it go like Google? Do Ministers take the view that a chap sitting in Cheltenham can learn more about citizens in Leicester than a bobby on the beat in Leicester? What sort of society does that become? This is a much broader conversation than just about who gets access to whose mobile phone location trace when.

The medium-term issue, which I think will become acute over a period of five to 10 years, is that the real problem is a diplomatic one. The real problem is about jurisdiction and how we get access to information in other countries, specifically America. America is where the world's data are kept. If they are kept in Finland or wherever because of cheap electricity, usually they are still controlled by a US company. There are some exceptions—Korea, Japan et cetera—but this is largely about how we get access to American data.

That means, like it or not—and many people are beginning to come to this conclusion—that the real fix for this is a cyber-evidence convention, like the cybercrime convention. That will involve diplomatic heavy lifting and an agreement, perhaps initially between America and the European Union, with other willing countries joining later as they wish, that provides a very much faster service for getting at stuff than the current mutual legal assistance treaties. For that to work, there are three things we almost certainly have to have. The first is warrants signed by judges, because that is what America expects. The second is transparency, which means that if somebody gets wiretapped you eventually tell them—when they get charged or after three years or whatever. The third is jurisdiction, because the real bugbear for companies like Google at the moment is that a family court in India gives it a warrant saying, "Please give us the Gmail of this person in Canada", who has never been to India. How do you simultaneously employ engineers in India and give privacy assurances to your users in Canada? That is why at present all this stuff gets referred to lawyers in Mountain View. That is the real problem, and it is time the Government faced up to it.

The Chairman: Professor Ryan, do you want to say something regarding an earlier point?

Professor Mark Ryan: I want to go back to the question of whether these are new powers or existing ones. Following what Dr Bernal said, one of the very huge powers that exists in the Bill is bulk equipment interference—that the state can interfere with people's computers on a bulk scale—which means that people who are not guilty of any crime, nor even suspected of any crime, may have malware put on their computers by intelligence services to collect vast amounts of data on innocent people in a kind of funnel, so that eventually criminals can be caught, but the people who are being subjected to that are not criminal at all. That seems to me to be an extremely dangerous thing in a free society. I do not think that the kind of oversight proposed in the Bill goes anywhere near being able to control that type of activity.

Professor Sir David Omand: The bulk equipment interference warrant can be sought only by the intelligence agencies in order to acquire intelligence relating to individuals outside the UK for the purpose of national security. For the sake of clarity, the Bill already restricts that.

Q83 Lord Strasburger: Sir David, your career was spent in senior positions in the Civil Service deep inside the security establishment, which probably makes you, of the panel, specially qualified to answer my question. It seems that over the past 15 years decisions were made behind closed doors to introduce several of the most intrusive and least overseen powers in this Bill without bothering to seek Parliament's approval. Why was it considered acceptable in a democracy to bypass Parliament and introduce large-scale and highly controversial surveillance powers without Parliament's explicit approval?

Professor Sir David Omand: I can only hazard an answer, which is that the legal regime under which previous Governments operated for the past 20 years, since the 1980s, was what I would describe as legal compliance; in other words, if it could be done lawfully under existing powers that Parliament had passed, Ministers would authorise such activity, after due legal advice, regardless of party—this is not a party political matter—in the interests of national security, the prevention and detection of serious crime, and economic well-being arising from causes outside the United Kingdom. That was the regime.

It was really when the Investigatory Powers Tribunal took the case and reported that the Government's activity, in particular GCHQ, might be regarded as lawful under the individual statutes but failed the rule of law test because it was not clear, as your question implies, to the public—

Lord Strasburger: Or to Parliament.

Professor Sir David Omand: Or to Parliament. This Government have taken that to heart, and the Bill is in part the result. We have moved into a new era and I am personally very glad of that. A lot of trouble would have been saved if, say, even five years ago the codes of practice—it would not necessarily have taken new legislation—on equipment interference, investigative powers and so on had all been updated to the modern digital world. For one reason or another that was not done. The shock of discovering what was happening, for very good reason—to defend the public and our security—was all the greater. I think the lesson has been learnt.

Q84 Victoria Atkins: I have a question for Professor Anderson and Dr Bernal. You talked a lot about privacy and, in particular, the debate in America about privacy. One thing that strikes me about the whole discussion is that very often we are focusing, if I may say so, on the worst-case scenario as to what the intelligence services and the Government will do with people's information. What are your views in relation to the computer companies that hold all this data about us? If we google a dating agency, Google will have that information. What are your views on those bodies, because to me they are very much part of the debate about privacy?

Professor Ross Anderson: Yes. I tend to take different views of different companies because of their different internal cultures. Having worked at Google, I understand and to some extent trust the culture there.

Victoria Atkins: You worked at Google.

Professor Ross Anderson: Yes, four years ago on sabbatical, so I understand it. My colleagues have worked for other companies. Fundamentally, whether you are a company that tries to be good or a company that is a bit less scrupulous, the underlying fact is that the modern economy depends on people trusting large service companies with their data, because it is so much more efficient to have 100 million people's data in a data centre than it is for everybody to be backing up their own hard drive at home and losing their photos and everything. That trust has to be maintained. If it is lost, the consequences could be dire for economic growth and the companies concerned.

People talk about worst-case privacy scenarios, but that is how people talk; that is how the media and politics operate—they operate by stories. The human brain is optimised for stories; it is how people remember stuff. If you get the perception out there that in the UK people who offer services have to leave a government back door, or remove the encryption if ordered, or whatever, it could be extraordinarily damaging for British business.

Victoria Atkins: Does selling people's data come into that? Are you comfortable with Google's position on that, having worked for it?

Professor Ross Anderson: Personally, I do not click on ads. If you want to go to a company that does not sell data, you can go to Apple or you can go to the trouble of having everything private. For example, I take the view that, if I am sending an email that I do not mind the FBI reading, I use Gmail; if I am sending an email that I do mind the FBI reading, I use something else. That is also the conclusion to which I think more and more users generally, and young people in particular, are coming to.

Q85 Matt Warman: I have a question for Dr Bernal primarily. As an example of new powers in this Bill, you said it was like following someone down the street and seeing which shops they go into. It strikes me that we have long had the power under certain circumstances for people to be placed under surveillance and followed down the street to see which shops they might go into. Could you give the Committee an example perhaps when we get back?

The Chairman: Order. There is a Division in the Commons, so we will adjourn for 10 minutes. I am sorry about that.

The Committee suspended for a Division in the House of Commons.

Matt Warman: To recap briefly, you cited the example of following a person down the digital street under authorised surveillance, which strikes me as a digital updating of analogue powers we have already. Could you offer the Committee an example that is not simply a digital updating of existing analogue powers and is genuinely novel because it is digital?

Dr Paul Bernal: It is a very important question, and there are lots of issues related to it. There are some things that we do in the real world, or the offline world, that we feel comfortable being observed doing. We have CCTV cameras in the streets, we have them in shops, and so on. We do not have them in our bedrooms, we do not have them staring at our diaries all the time and we do not have them monitoring exactly where we walk. We get the choice: do we want to go to this place where we know there is CCTV, or that place where we know there is not CCTV? That is one of the important differences.

The thing about the Internet as it is now, particularly for younger people, is that they do literally everything on it; there is no aspect of their lives that does not have an online element. If you have a system as is proposed with Internet connection records, for example, where there is some gathering of their entire browsing habit, not beyond a certain level—I hope we will get on to Internet connection records later—at least you have knowledge about what they are doing in every aspect of their lives. When you go to the doctor, you expect confidentiality from your relationship with the doctor when you discuss your health issues. If you visit a website to research a particular health condition, that may reveal just as much about you as you would reveal to your doctor—in fact, many times more than you might reveal, because people have a sense that they can get more intimacy by doing things on the Internet than they might even be prepared to admit to a doctor.

There is another element. We talked a little about Google and others. Given the way profiling works for almost all commercial Internet companies, and the way big data analysis works, you can draw inferences from relatively small amounts of browsing data that can then be used to infer stuff that you would otherwise keep private. An example is your sexuality. You might not want to reveal your sexuality, but big data can make a probable analysis of it with a relatively small number of places you visit on the Internet.

It goes back to the question about whether we are looking at extreme cases. We are looking at extreme cases in some ways, but we are also looking at very ordinary cases. What we all do on the Internet has an impact on credit ratings, insurance premiums and things like that. They can be based on very basic information that can be gathered about how we behave.

I am sure David will say that safeguards are built into the Bill so that it can be used to do only certain things, but that is not really the whole story for two reasons. One is that data, wherever they are and in whatever form, are vulnerable in many different ways. The example that comes most readily to mind, because it is so recent, is TalkTalk having been hacked, and holding exactly the kinds of records that we are talking about. That information is ideal for ID theft, credit card fraud, scamming and things like that.

If we gather those Internet connection records, we are basically creating a very targeted database, which says on the front, "Hack me, please, if you want to get ideal information for these kinds of crimes". We need to be careful not just about what we think the Government are going to do. Like David, I trust to a great extent our security services and police, but we are creating something that can be misused by other people, not just by them. There are many ways in which that can happen.

Q86 Suella Fernandes: In terms of legality, the issuing of warrants is subject to the test of it being necessary and proportionate. In light of that, what is your view on its compatibility with proportionality as required under the ECHR?

Professor Sir David Omand: Proportionality and necessity are in the Bill. They are written in, as they are in the current legislation. Dr Bernal's examples were very good ones of why digital mass surveillance is a thoroughly bad idea. Thankfully, it does not happen now, and under the provisions of this Bill it could not happen in the future either. The question that I suggest the Committee really needs to address is how proportionality is assessed—precisely your question—not just in relation to the granting of a warrant but the whole process through which the selection of material for examination by human beings—the analysts—takes place. The IPT, the independent court, has examined this; senior judges who oversee interception have examined it, and they are satisfied that the current procedures are consistent with the Human Rights Act, Article 8 and thus respect privacy. Equally, there is no reason why the provisions cannot be applied in practice in ways that remain consistent.

The decision on proportionality and necessity rests with the person signing the warrant. The Home Secretary has made her view clear in the Bill. I am disappointed that she decided that she had to sign police warrants and that they would not go direct just to the senior judge for approval, which was our recommendation in the independent review commissioned by the former Deputy Prime Minister, and that would be more consistent with David Anderson's review. I strongly believe that the Home Secretary or the Foreign Secretary, as appropriate, should sign the warrants relating to national security and the work of the national intelligence agencies, for which they are statutorily responsible to this House. The police service is in a different constitutional position, and I would have thought that purely police matters could go straight to the judge. It is no harm that the Home Secretary signs as well; it is just additional work.

Dr Paul Bernal: Can I go back to the question of proportionality? One of the key things is not just about the warrant to access the information. One of the key elements of proportionality is the gathering and holding of the information itself. The CJEU has consistently—even more so recently—held that the holding and gathering of the data engages Article 8, and that indiscriminate generalised holding and gathering of data is contrary to fundamental rights. That was held in Digital Rights Ireland; in the Schrems case it was part of the key reason why the safe harbour decision was invalidated. This is not because they have some perverse view that does not match with reality but that the European Court has started to understand the impact of holding all this personal data. It is not just the warrants—to a degree, I agree with David about the warranting process; it is the gathering of the data that I disagree with, particularly the way Internet connection records are set out. All this data seems to me to be gathered on the assumption that that is

all okay and it is just the accessing we need to deal with. I cannot see how this law would survive a challenge in the CJEU on that basis.

Professor Sir David Omand: I very strongly disagree. I am not a lawyer, but it seems very clear to me that the Schrems and the Digital Rights Ireland judgments do not bear on the point that has just been made. Those judgments did not consider the question of proportionality of collection and selection, which is not indiscriminate collection of data willy-nilly. You might want to take advice on that.

Professor Mark Ryan: I want to comment on the bulk provisions of the Bill, because they allow for the collection and automatic processing of data about people who are not suspected of any crime. Therefore, I do not think it is correct to say that this is not a recipe for mass surveillance. It is the processing of data about everybody, and in my opinion that is mass surveillance.

Professor Sir David Omand: But it is not processing data about everybody.

Q87 Baroness Browning: We have covered quite a bit of my question about definitions. Clearly, we have differing views on the panel. Sir David, in your evidence to the Science and Technology Committee I believe you suggested that somehow you would never get a perfect definition, and in the absence of that a pragmatic approach should be taken. Do you want to identify the balance between being safe and being practical?

Professor Sir David Omand: The starting point has to be the value of communication data both to the police and to the intelligence agencies. The police evidence is very clear. It has huge importance in ordinary crime as well as in countering terrorism and cybercrime. From that starting point, we have to have an authorisation process that can cope with the number of requests, which is over 500,000 a year, so talking about requiring warrants to be signed by Secretaries of State or senior judges is not appropriate. The justification for that was that it is less intrusive to look at communication data than to look at content, and that principle is reflected in the Bill.

The point I was making to the Science and Technology Committee is that there will be some hard cases, and Professor Anderson gave some examples of precisely that. If you move the cursor too far over to be so restrictive, you create a real problem about the authorisation of data communication requests. If you move it too far the other way, you get the equal and opposite problem of not sufficient authority being applied. The cursor is more or less in the right position, because it has taken the RIPA 2000 definition of who called whom, where and what, and transferred it to the computerised age of which device contacted which server up to the first slash of the address, but there will be hard cases. I was suggesting to the Committee that you have to be pragmatic and ask whether the overall public interest in the authorities and police having this information, which is vital for upholding the law and bringing people to justice, balances the fact that you may occasionally have a hard case. In my view it certainly does.

Baroness Browning: If we get the definition right and if we get the clarity that the panel seems to feel is lacking at the moment, do you think that will serve us for now, or will we have to keep revisiting this?

Professor Sir David Omand: For the sake of clarity, I think the definitions are clear; it is reality that is fuzzy. The parliamentary draftsman has done a very good job trying to clarify this. I am not sure you can make it any clearer.

Baroness Browning: That is very clear. Thank you.

Dr Paul Bernal: This is a really important element. Sir David said that communications data was less intrusive than content. I do not think that is true. They are differently intrusive. There are several reasons communications data can be more intrusive. One is that it is by its very nature more suitable for analysis and aggregation. You can do more processes to it than you can to content. That means that it is subjected to what we loosely called big data analysis. It is also less hard to disguise in some ways. You can talk about a coded, not encrypted, message to somebody. In England we do this all the time; when we say "quite", it could mean a million different things depending on the context. You cannot do that so easily with communications data. That means that sometimes you can get more information out of communications data than you can from content. I do not think you should be under any illusions that somehow it is okay to have as much communications data gathered as possible but not okay to get content. They are different things. For individuals, sometimes content matters more; en masse, communications data matters more.

The Chairman: Before you came in we were discussing the differences between communications data and content, but the drafters of the Bill and the Government who sponsored it seemed to indicate that there is a significant difference in terms of people's privacy with regard to what is written by them and to them, as opposed to the hows, the wheres and the whens, but you are contesting that.

Dr Paul Bernal: I am contesting that. I would say that it can be worse. You have at least some control over what you write, whereas for communications data largely you have very little control over it at all. It is a different sort of intrusion.

Q88 Baroness Browning: From the point of view of the speed at which things change, could you indicate whether you think that even if we had an imperfect definition, in your terms, we are going to have to keep coming back to legislation more quickly to update it? Is that a danger?

Dr Paul Bernal: Frankly, yes.

Baroness Browning: Do you think we will keep coming back to this?

Dr Paul Bernal: I think you will be coming back to this and you should be, because things change in so many different ways. This is not the sort of law that you can set down and say it will last for 15 or 20 years without amendment, because the technology is moving too fast; people's behaviour is changing too fast.

Baroness Browning: May I bring you back to Sir David's point? Seeking perfection is perhaps something that we should compromise with pragmatism.

Dr Paul Bernal: You should, but you should compromise it by adding extra oversight rather than by accepting a loose definition, by making sure you can monitor what the intelligence and security services and the police are doing so that pattern of behaviour matches the intent behind the law as well as the definition. This is part of Lord Strasburger's analysis of how powers have grown without parliamentary approval. It is very easy and we have seen it historically again and again. People have not been watching what is going on and you need to continue to monitor things. I am not yet convinced that the oversight arrangements here are strong enough to do that. The idea of, if not a sunset clause, a revisiting clause of some kind might be worthwhile, and also monitoring the monitors: how are the oversight arrangements working?

Q89 Stuart C McDonald: Turning to communication service providers and the requirement that could be placed on them to store up to 12 months' worth of communications data and Internet connection records, how feasible is it for providers to do that?

Professor Ross Anderson: It could be extraordinarily difficult and expensive if they are to do what they are advertised to do. We are told that Internet connection records will enable the agencies and police to get past what is called carrier-grade NAT, which is a technique whereby the IP address of your mobile phone might be shared with 1,000 other mobile phones, the idea being that, if someone does a bad thing online on Monday, you ask O2 and they say that it could be any one of 1,000 phone numbers, and, if the person does another bad thing on Wednesday, you have another list of 1,000 phone numbers and you say, "Aha! The common number on the two lists is this one". It is not going to work that well, first because you will find hundreds of common numbers on the list; and, secondly, if you want to relate that to things people have done on other service providers, you have to relate it to an ID on Google, a handle on Twitter or a logon for Facebook. For that, you would have to require the communication service providers to store very much more data than they do at present. You would have to get them to store precise time stamps, addresses and so forth, which they will not do.

ICRs will not work as advertised. What they will do is create an extraordinary capability power for investigators to say, "Show us all the websites that these two bad people have visited in the past month and all the other people who have visited the same websites". If you want that capability, which appears to be what is intended, you end up requiring lots of people to store lots of stuff. There is, first, the issue of cost if you are to remunerate communication service providers in Britain; and, secondly, there is the likelihood that service providers overseas will refuse outright because it would be too much effort and energy to redevelop their systems, and Britain is only 4% of the market anyway.

Dr Paul Bernal: The Danes are the people who have got closest to doing this, and I would recommend, if you can, to get one of the witnesses from the Danish abandoned attempt. They ran it for nearly seven years and got almost no useful information out of it, but there was a huge cost, even though they were warned beforehand by the ISPs, as I believe they will be here, that this is not a practical proposition and is not likely to be an effective one.

Professor Sir David Omand: The Committee will discover, if they do that research—I hope they will—that the model the Danes chose is not the model I strongly suspect the

Home Office would choose. The Danes themselves are revisiting it at this very minute because they may find post-Paris that it is necessary to go back and look at it.

Q90 Matt Warman: I want to talk a little about encryption or decryption. Do you think it is reasonable for Government even to ask communications providers to provide unencrypted material for something that is currently encrypted?

Professor Ross Anderson: There is a power in Section 3 of the RIP Act which allows them to do that. As I remarked earlier, Parliament saw fit to hedge it with very stringent safeguards. Nowadays, it would be much more difficult, because many service providers encrypt stuff by default. They do so not out of any particular malice towards agencies but simply to stop other people stealing their ads and customers. It has just become the commercial default; it is what everybody expects. With messaging services, everybody increasingly expects stuff to be encrypted end to end. The Government of Kazakhstan have recently decreed that everybody has to install the Kazakhstan Government's cert on their machine from 1 January. I predict that if you have an iPhone in Kazakhstan you will suddenly find that none of the services works. That will be worth watching.

Matt Warman: Sir David, do you have any thoughts on whether we are likely to get anything meaningful out of demanding unencrypted data from people who currently encrypt it anyway?

Professor Sir David Omand: Of course, you will be distinguishing between content data and communications data, which clearly has to be delivered in a form in which the authorities can use it. If we are looking at content data, as far as I can see there is no back-door encryption provision in the Bill. The Government have said that they are not seeking it. I know the agencies are not seeking it, so as end-to-end encryption spreads it will get harder and harder for the authorities to be able to access unencrypted content, even for their highest priority suspects. That is a fact of life.

Does that mean that the authorities should have no power to seek such information, and to do their best in cases where it might be available? That is the approach I would commend to the Committee. It is a power to seek, but I do not think it is in Parliament's power to insist that all encryption can be bypassed, nor would it be a very sensible thing to ask for in terms of the national economy and the need for the Internet to be secure. There will be specific cases where it will make sense and information could be made available, and the Bill should provide for that.

Matt Warman: To be clear, in general you do not see the Bill as providing the back door that people have spoken about.

Professor Sir David Omand: No, I do not.

Dr Paul Bernal: Many of the companies concerned do not share Sir David's view, and that is one of the reasons why some of them are distinctly disturbed by news of the Bill. One other thing that we need to be very clear about—Professor Anderson has already referred to it—is that we do not want to put British companies at a disadvantage, because they are more likely to be subject to the force of British law than a company in California

or Korea. If we put the power in place to allow them to do it, they are disadvantaged, and that is not good for anybody.

Matt Warman: Which only emphasises the need for clarity, does it not?

Dr Paul Bernal: Clarity is what is needed.

Q91 Matt Warman: To move on to equipment interference, what does the panel understand that to be?

Professor Ross Anderson: It is basically hacking or the installation of malware, or what the NSA calls implants and what we call remote administration tools in a machine. If I am a bad person, the police would be able to say to O2, "Put an update on the android on Professor Anderson's phone", and that would enable them remotely to turn it on, use it as a microphone or room bug, or look at me through the camera, collect my location history and all the rest of it. What is more, as we get digital stuff in more and more devices they could do the same to my granddaughter's Barbie doll; they could do the same to your car or your electricity meter. It is open season on the Internet of things. It goes without saying that the controls around that need to be very carefully drawn; otherwise, it undermines trust. If UK producers of stuff can have their arms twisted to provide a capability to put implants into stuff, why should people buy stuff from Britain?

Professor Sir David Omand: I agree with the point Professor Anderson makes about the need for careful oversight of this, but the power already exists; it is already in use under existing statutes, including the 1994 Act. It is of inestimable value to the intelligence agencies, particularly on national security addressed to targets overseas where there are legitimate demands for intelligence. Some 20% of GCHQ's output benefits from that kind of technique. There is nothing very new about it.

Dr Paul Bernal: There is nothing new about it, but there is something new about our behaviour and the technology we all use. Twenty years ago I was not using anything that was encrypted at all; now half the stuff I have on my phone is encrypted by default, and another batch is encrypted by choice by me, so for normal people this now becomes relevant when it was not relevant before.

Professor Ross Anderson: What is new is that we found out about it thanks to Edward Snowden, and GCHQ admitted that it was doing it just in the last month or two, thanks to the case currently before the Investigatory Powers Tribunal. People are beginning to get worried about it, and with due cause.

Q92 Lord Strasburger: Gentlemen, can you help me out with bulk personal datasets? The Bill and the Explanatory Notes are very vague about that. The ISC report was rather vague about it—it was hugely redacted. The Home Office will not tell the Committee the identity of the databases it is scooping up, so it is very difficult for this Committee to assess the proportionality, risks and intrusiveness of the collection of bulk personal datasets. Does anybody know what they contain? Do they contain medical records? Do they contain bank records? What do they contain?

Professor Ross Anderson: For starters, we know that the police have access to things like credit reference and DVLA records. That is public knowledge. Secondly, they have access to medical stuff. They have had that since 1996. At the time, I happened to be advising the BMA on safety and privacy and that sort of thing came through. Thirdly, in any case, hospital medical records were sold on a wide scale in the care.data scandal last year, and it would have been rather negligent if GCHQ had not grabbed a copy on its way past. Fourthly, it is well known that some kinds of bank records, in particular all international financial transactions, are harvested on their way through the SWIFT system.

Professor Sir David Omand: Not true.

Professor Ross Anderson: This has been a matter of enormous contention in the EU and elsewhere. It is only to be expected. If I were, for example, an investigator for the FCA, I would want everybody's bank statements too.

Professor Sir David Omand: Chairman, it is important not to allow fantasy to intrude at this point. The central bank governors responsible for the SWIFT system agreed that that system could be searched for specific transactions of known criminals and terrorists. That is public knowledge. All SWIFT data is not scooped up.

Lord Strasburger: Perhaps we could impress on the Home Office the need for the identity of these databases to be revealed.

The Chairman: That is something that we would have to do in private session, but I take the point that there is a serious difference of view between the witnesses on what is a hugely important subject.

Q93 Dr Andrew Murrison: I am going to be fairly brief, because I think we have covered quite a lot of this already. I refer to the international dimension. We sit here thinking we can make various laws and regulations, but we are talking about a global industry. Referring to some of your previous comments, could you reiterate the likely reaction of the international community to the Bill, in particular the feasibility of gathering ICRs, given that it is entirely in the gift of companies whose headquarters are not in the UK?

Professor Sir David Omand: We took evidence on this as part of the independent surveillance and privacy review run by RUSI and we got a variety of answers from international and British companies. Some of the companies said that as a matter of corporate social responsibility they wanted to be in a position to provide this kind of information for the purpose of preventing serious crime and terrorism, but they felt extremely nervous about doing it without a firm legal basis on which warrants or authorisations would be made. Other companies said that as a matter of company policy they did not believe their data should be made available to any state or law enforcement authority. You have a variety of views. The provisions of the Bill, which include the provision that the Home Secretary can make judgments about what it is reasonable to expect, will be partially successful; but they will not be completely successful, because some companies will simply refuse, and I cannot see the British Government attempting to launch civil actions against major players.

Dr Andrew Murrison: Presumably that means that the disinclined would note those who were complying and those who were not and go for those who were not.

Professor Sir David Omand: The intention is not to make public the companies that comply and those that do not.

Professor Ross Anderson: We all know the companies that will comply. They are the ones that get large amounts of their revenue from Governments, or that rely on Governments for capture regulators—companies such as IBM, BT and those set up several generations ago. Companies that have been set up in the past 20 years think differently because they have a different culture—the Silicon Valley culture. Their money comes either from their users directly or from advertising—from their users buying stuff or being advertised to—and they take a completely different view. It is not much good getting BT on board if all BT is doing is providing a piece of copper wire from people's houses to where the real action starts, so it is the view of the big American service companies that matters more than most. They are going to drag their heels.

There is the issue of foreign Governments. There is also the issue of what happens to small start-ups in the UK, which is absolutely crucial. For example, about five years ago one of my postdocs set up a security start-up. Because of the arm-twisting that the agencies have always indulged in, he decided to set up a coding shop in Brno in the Czech Republic. More and more people will be doing that, simply as a matter of default. You cannot run a tech start-up nowadays unless you have a marketing operation in North America, because that is where you make your first sale and most of your initial sales. If we create a regulatory regime where it is only common sense for people to put their coding shop, their engineering, in North America, Seoul, Mumbai or wherever, the cost to us directly or indirectly down the stream of time will be huge.

Dr Paul Bernal: We have to be aware of where things are moving. There may be a number that are co-operating willingly now, but that will shrink. More and more companies are likely to say, "No, we are not going to give this", and they will be the bigger and more successful ones. You make yourself a hostage to fortune by assuming that this will end up functioning.

The Chairman: Thank you very much indeed. I thought the whole session was absolutely riveting. You have given us an enormous amount to think about. Obviously, you have very different and varying views on the issues before us, but you highlighted issues that very much need highlighting. I know that members of the Committee are grateful to all four of you for giving us your very robust and significant views on this important Bill. If you would like to add any written evidence to supplement what you have said, we would be more than happy—indeed delighted—to receive it. Thank you very much indeed.

Witnesses: Lord Blunkett and **Mr Owen Paterson MP**

Q94 The Chairman: We give a warm welcome to our colleagues, Lord Blunkett and Mr Paterson. First, we apologise to you. It is largely the fault of the House of Commons; it decided to have a vote and that put the whole business on by about 15 minutes. We are

extremely grateful to you both for coming along to talk to us about this very important Bill. Because of your experience in government, both of you know a great deal about the issues involved, so we are very grateful indeed. I will take advantage of my position as Chairman by asking the first question, which is for Lord Blunkett and for Mr Paterson. It is a very simple one. Is this Bill necessary, in your view?

Lord Blunkett: I cannot promise to be anything like as riveting as the last session, Chairman. Could I declare a non-pecuniary interest? I have an interest in a company that is involved in verification and authentication in the payments business, so I have a bit of knowledge—not as much as your previous contributors, obviously—about what will drive companies out of Britain.

Yes, the Bill is necessary. It required updating, for the reasons that I spelt out in my written and oral evidence to the ISC, and if people have insomnia they are very welcome to read it. I will not repeat all that, except to say that we have moved from an analogue to a digital age. For some time, we have needed to update the former telecommunications procedures and safeguards for the age we are in at the moment. My precept has always been that we use the same principles. When I hear people suggest that somehow there is an issue with holding telecommunications data long enough to be able to access it when necessary, or that it is the same as the content, I wonder whether they would have used the same arguments if we were discussing this 20 years ago, in the telecommunications age that existed then.

The Chairman: Thank you very much. Mr Paterson, is it necessary, in your view?

Mr Owen Paterson: Chairman, thank you very much for inviting me to your Committee. Yes, I think that broadly it is, to bring the powers that our agencies have up to technological speed with our opponents. Having worked in Northern Ireland, as you did, I have no doubt of the real dangers posed to our citizens on a daily basis. It is only right that we give the incredibly brave people who work in our security agencies every necessary tool in order to beat them. I totally agree with Lord Blunkett. The original principles should always prevail in how we oversee and manage this intrusion.

Q95 The Chairman: Before I move on to colleagues so that they can ask about interception and authorisation, which both of you are very knowledgeable about, I have one more question. A lot of the Bill covers bulk interception, bulk acquisition of collection of communications data and bulk equipment interference. Do you think that an operational case has been made for that?

Lord Blunkett: The term "bulk"—people talk about metadata—provides a fog around the issue. Surely the fundamental issue is that what is taking place requires monitoring. If monitoring involves collection of data, where should those data be held? Six years ago, the Government backed off the idea that there should be any attempt to hold centrally, so we are asking the private sector to co-operate. We are doing so in a way that allows the agencies to be able to do the job. We need to demystify this, if I may say so, because the term "bulk" worries people. The fundamental issue, which was touched on in your previous session, is what in a practical sense can be undertaken, and what meaningful information can be gleaned from it for acceptable purposes. If we drill down to that, we

start to demystify it and can then challenge the agencies as to whether what they are doing is relevant to the objective that we have laid out for them.

Mr Owen Paterson: I broadly agree. Once the principle of interference and capture of private data is accepted, I am not worried whether it is a small amount of data or whether it is a bulk amount of data—which, as Lord Blunkett said, has become a bit of a shibboleth. The principle must be that this data are managed in a responsible manner. In my experience, our services have been punctilious in the manner they respect the constraints and the protocols put on them.

Lord Strasburger: On the subject of bulk, is it not true to say that the concern is not necessarily about the quantity but about whose data are being captured? There is a difference between surveillance or interception of the data of suspected criminals or terrorists and surveillance or interception of those of the rest of us. It is targeted against untargeted, rather than bulk against small.

Lord Blunkett: We have always collected them. They have been collected, have they not? They have been held. The records have been there, under the old telecommunications system. They were not accessible in the same fashion as they are now, at the speed they are accessible. Collation is possible, with new technology addressing new technology, but the process was the same, was it not? The data was held.

Lord Strasburger: It was not quite the same. In the case of telephone data, the data was held by the telephone companies for their own billing purposes. In the case of Internet connection records, we are asking the ISPs to create the data, which do not currently exist.

Lord Blunkett: We need, perhaps, to ask the ISPs, as you are presumably doing, what they do with the data, because the idea that they hold them now only for billing purposes is mythical. The amount of data that is used by ISPs for all sorts of purposes—people seem willing to provide and to collaborate with that—is enormous. Just ask how much a Sky box provides, if we consider what is done with it afterwards.

Mr Owen Paterson: We are broadly in agreement again. Huge amounts of data are kept on every one of us, every day. It is the manner in which those data are used—whether they are used responsibly and whether we have the right protocols to control that use of data—that worries me. That is the main concern.

Q96 Mr David Hanson: You have both exercised the authorisation of intercept warrants, in Northern Ireland and in the Home Office. Could you give the Committee a flavour of how urgent those requests were, how often you turned them down and whether there were any detailed issues—without referring to cases—that you think the Committee would wish to reflect on in relation to the existing authorisation procedure? Perhaps you would like to answer, Lord Blunkett. I can see Mr Paterson passing over to you.

Lord Blunkett: I am happy to do so; I was just trying to share the burden a little. Let us try not to exaggerate. Many of the warrants authorised—there are probably slightly more now than there were in my day, but there were about 2,500 a year—came through on a process of sensible authorisation, which gave time to look at the detail. They were often renewals

of authorisation previously given, on a three-month basis, and then more frequently after that.

There were occasions when it was absolutely vital for the services to have an answer in the middle of the night. I am trying not to exaggerate it, because this is not about theatre—it is about reality. On more than one occasion when I had switched off my mobile phone and was not at home, I was literally dragged out of bed by the protection team. When you get one, you have to do it there and then, although in the middle of the night you are not as compos mentis as you might be and you question whether you should pause, drink a coffee and make sense of it. As a whole, it was necessary to be able to turn them around speedily. I know from the questions that Owen has raised in the Commons that both of us are concerned that on critical occasions an incident cannot occur because an authorisation has been delayed.

You asked me a second question: how often did I turn down requests? Out of the numbers we are talking about—I have thought about this a lot—I would say about 2% or 3%. Some of those then came back with further information and clarification that helped me to see that they were necessary.

Mr Owen Paterson: When I arrived at the Northern Ireland Office, it was quite a delicate period. Your Government had just got devolution of policing through. Sadly, there was an element of the republican community that was completely determined not to accept the settlement and wanted to continue physical violence and terrorist actions. They were extremely dangerous. Sadly, we had to ramp up our activity, to get quite a lot of extra money from the Government and to re-equip certain agencies.

I was very aware that we were fighting a 24-hour campaign. One of the first things that I did on day one was to make it very clear to my private office, "This is a priority for me. You wake me and interfere with what I am doing at any time. Never, ever, put my private convenience before speed in bringing one of these requests for a warrant to my attention". The vast majority were done in an orderly manner. We had diary slots once or twice a week; I cannot remember how many. As David said, they were frequently repeats. Sadly, it was the same old names coming round and round every three months. As David said, occasionally I would be woken up at 2 or 3 o'clock in the morning and asked for a very urgent decision. That is what has provoked me to make public comments that I am extremely concerned about some of the proposals in the Bill that might interfere with swift executive decision-making.

On the number that I turned down, I am with David. It was a very small number, but I did. It was known that I was not a patsy. I turned down the ones I was not satisfied with, or I sent them back for further information.

Mr David Hanson: That leads to two questions, which both of you can answer. First, how do you now feel about judicial oversight of that process? Is it fair, proportionate and the right thing to do? Secondly, given the concerns that Mr Paterson has raised publicly in the Commons, is there a definition for you of the turnaround time in an urgent case for any judicial oversight commissioner who may be appointed under the Bill?

Lord Blunkett: I am happy with the compromise—I suppose you would describe it as the sophistication—if the process of review is in tandem with the Secretary of State's decision-making process. Historically, judicial review is exactly what it is: a legal and administrative review of the way in which the Executive or their agencies use powers that have been granted to them. In our present process of commissioners, it is down the line when the process is reviewed and checked. This would mean that every decision would be subject to that tandem process. I would be unhappy with it if it cut out the Secretary of State, and those who are vehemently against any kind of intercept and surveillance measures would be horrified if there were not some sort of review now. We are trying to get that in tandem.

Mr David Hanson: It is more approval than review.

Lord Blunkett: That is the debate you are having—to clarify what it is. If it is not a review, are the commissioners being reviewed down the line? There is a presumption in our present political environment that judges know better than anyone else and are better than other people at all sorts of processes. I think that they are very good at interrogating and being able to make judgments in the critical judicial system that we have. I do not think that they are any better or worse than senior politicians at making a judgment on whether the evidence placed before them in these circumstances stands up. If I may be controversial, Chairman, because you have been through it yourself, sometimes you weigh the evidence and use instinct. Instinct is no less valid from those who have come through years and years of the political process and have been publicly scrutinised themselves than it is from judges.

Mr Owen Paterson: I would go further than David. I am wholly in favour of strengthening the review procedure after a decision has been made. Whenever I signed one of these things, I was fully conscious that I was subject to quite a rigorous inspection in the cold light of dawn, possibly some months later. I was fully conscious that I could be summoned to a Committee like this and could be hauled up on the Floor of the House of Commons in Questions. There was a real responsibility. However, I really believe that it is vital that the decision is made rapidly by a Secretary of State with full executive powers of decision-making. It is up to the Secretary of State to make a decision, often under very imperfect conditions and with imperfect information. As David has just said, often you may have to trust instinct. Our current Home Secretary has done it for five years and is extraordinarily well-placed to make difficult decisions. I wholly fail to see the value of distinguished judges coming in and taking part in the decision. I really oppose it. Go back to Montesquieu and the separation of powers. Their skill is interpreting law or, here, interpreting the manner in which a law has been put into action by an Executive. I feel very strongly that these are executive decisions. They are operational decisions and must be made by a democratically elected Minister, accountable to Members of Parliament.

Mr David Hanson: This is the final question from me. The key element will be the interface between an urgent request to you as the Secretary of State for one or both departments versus a judge reviewing that decision and taking a different view on an urgent case. Where does responsibility lie in the event of that type of conflict?

Mr Owen Paterson: This is what worries me. I stressed in my opening comments that often a swift decision needs to be made. The Secretary of State will be very conscious of his or her responsibility and will make that decision. Here you have a second body party to the decision. Clause 138(3) states, "Where a Judicial Commissioner refuses to approve a decision to issue a warrant under section 137, the Judicial Commissioner must give the Secretary of State written reasons for the refusal"—written reasons. How will that work if the Secretary of State for Northern Ireland is in one place, the commissioners are in another and there is information that may have come from our allies in the Garda Siochána that an operation is under way?

The pass on this has partly been sold. There is the equivalent of an emergency provision, where the commissioners have five days to make a decision. Frankly, that could apply to everything. I would be happy with that. I am perfectly happy to have more judicial scrutiny, more frequent review and more regular meetings with the relevant Secretary of State. They came to see me probably once every six months; you could do that much more frequently. I am very strongly opposed to a member of the judiciary making a co-decision. That is really dangerous. What happens if it goes wrong? Who is to blame? Who comes before Parliament? Who do the relatives sue if a bomb has gone off and a Secretary of State had made a valid decision, under difficult circumstances, with imperfect information, but it had been skittled by a very well-meaning, very well-trained judge on a legal nicety? This has not been thought through. Do they get together in the middle of the night and look at the written review? Do they then together go back to the agency and ask for more information in the middle of the night?

It has not been thought through. I see delay and muddle. There has to be a difficult decision, made by an elected Minister, who is subject to intense scrutiny after the event. This muddles the role of the commissioners. If they are to be a serious body, reviewing and scrutinising, they are compromised if they are active in this decision. It will go one of two ways. Either they will become patsies, to use my earlier phrase, and will just go along with the Secretary of State, so they will be devalued, or they will become an extra body that is not accountable to Parliament. Either of those results is very unsatisfactory. To make it even worse—to get you depressed—it is much worse in Northern Ireland, where you have divisions among judicial bodies, as we saw with the Duffy case collapsing only last month.

Q97 Victoria Atkins: My question has been answered by both of you. The question is, who judges the judges under this format? Please correct me if I am wrong, but there is no accountability for the judicial commissioners, whereas the Home Secretary is accountable to the House of Commons and Select Committees in this place.

Mr Owen Paterson: As I said, I am very concerned that these judicial commissioners will not be accountable. Then there is a third human being with the powers of Solomon, according to the Bill, called the Investigatory Powers Commissioner. If you look at the same clause—Clause 138—subsection (4) states, "Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to issue a warrant, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant". That introduces a third body, with more muddle, more delay and more lack of accountability. I go back to my comments to

David Hanson. What happens if it goes wrong? Who is to blame? Who is hauled up before this Committee? Who is hauled up before the Northern Ireland Affairs Committee for letting an operation that could have been stopped go ahead, when the democratically elected Secretary of State had made a clear decision? I am not at all relaxed about these proposals. I really do not like them.

Lord Blunkett: I share Owen Paterson's genuine concern, but I also know, with a political hat on—this is why your Committee has a massive challenge, but why it is sensible to have scrutiny of the Bill in this way—that we need to find a way of ensuring that a tandem process can work, simply because there is an atmosphere now, driven by those who suspect the state of all sorts of things, that makes it very difficult to resile from what has been put forward. Sophisticating it will be the challenge. I would like to wish you luck with that.

Dr Andrew Murrison: Answerability is an important concept, but what does it mean in practice, since Secretaries of State answering on warrantry issues will invariably say, "We do not comment on security matters"? The other point, just for observation, would be the stance taken by the rest of the "Five Eyes" community in relation to judicial oversight, which, even under the Bill as it is currently drafted, is quite different. Do you think that there may be scope for separating warrantry on criminal matters from warrantry on national security matters, removing the Home Secretary from the former?

Lord Blunkett: The problem we have had with authorisation is that the more dangerous the individual or individuals, the more likely it has been that the Secretary of State—or, in the case of criminal behaviour, the Home Secretary—has been dealing with it. We have had almost a perverse situation where the police—obviously you will look at this separately, but I said it in my evidence to the ISC—have been able to get authorisation to do things without going to the Secretary of State. I think that we have it the wrong way round. The Secretary of State should be responsible for the warrantry, for the reasons you are very familiar with. You cannot separate serious crime and the danger of terrorism, not least with interconnection, money laundering and everything that you were debating before we came in.

Dr Andrew Murrison: Would it be a little easier if we had a proper definition of national security, which we do not have on the face of the Bill at the moment?

Lord Blunkett: We have all sorts of articles in relation to exemptions, do we not, within the European Union—I dare not mention it in Owen Paterson's presence—as regards definitions? Earlier Sir David Omand indicated that we have got as near to it as possible, in an imperfect world.

Mr Owen Paterson: Could I add one or two comments? First, I do not entirely agree that Secretaries of State just bat off these questions and say, "It is not appropriate to reply". When serious incidents happen, often there are quite major investigations and what went wrong comes out. This will happen only when something goes horribly wrong, so the process will be exposed.

On the issue of criminal or terrorist issues, I totally agree with David Blunkett. In Northern Ireland, where you cross the line between excessive fuel smuggling, racketeering and drug smuggling feeding violence, which may be criminal or terrorist violence, it is a pretty grey, woolly area. Both those came across my desk, and I did not differentiate.

Q98 Suella Fernandes: I have two small questions. You have talked about the notion of instinct that Ministers may have when issuing warrants that the judiciary may not possess and said that it is an important factor to preserve in the decision-making process. Could you say a bit more about what distinguishes the ministerial perspective on such decisions from a judicial approach?

Lord Blunkett: The judicial approach would obviously get there, because after time they would be familiar with the process. That happens to Secretaries of State coming in, but on the whole you do not get people who are inexperienced in the general areas who are Home Secretaries, Foreign Secretaries and Secretaries of State for Northern Ireland. They are still learning when they come in and when they are doing it, as we all are when growing into jobs. I am sure that, after a period of time, those who have been schooled and have undertaken their process of promotion in an entirely different way would come to expect to have to use instinct, but it is not helpful to a judge to use instinct, is it? Judges are not trained to use instinct. They are trained to resist using instinct, are they not, at least theoretically? The facts have to be dealt with, even if the judge believes there is a problem. All I am saying—I am trying to be honest about it—is that you examine the material that has been put before you and do everything that you can to stick to that, rather than what you feel about it, but there are occasions when you think, "I will go with it. My instincts tell me that there is something entirely right about the application and entirely wrong about what these people have been doing".

Suella Fernandes: Would you say that it is a wider perspective, as opposed to a narrower legal perspective?

Lord Blunkett: Inevitably, yes. If it was only a legal matter, you would not have that process at all.

Mr Owen Paterson: That is exactly right. If this was nice, rinky-dinky, clean and tidy, you would not need politicians. You would have these wonderful judges who were all knowing and all knowledgeable, who interpreted law that told them exactly what to do and who did not move an inch off it. If you look at Clause 169(5) and (6), they are expected to make political judgments. It says, "In exercising functions under this Act, a Judicial Commissioner must not act in a way which is contrary to the public interest or prejudicial to—(a) national security, (b) the prevention or detection of serious crime, or (c) the economic well-being of the United Kingdom". The judicial commissioner must ensure that he does not "jeopardise the success of an intelligence or security operation or a law enforcement operation … compromise the safety or security of those involved, or … unduly impede the operational effectiveness of an intelligence service, a police force, a government department or Her Majesty's forces". Every one of those requires a difficult political decision. There might have been information from Dublin that someone is on the way up. Someone else is coming in from Donegal. You do not have perfect information. You have to trust the information you have been given and you have to make a subjective

judgment. You are fully conscious that you might be up for very severe scrutiny—in my case, some months afterwards—in the cold light of day, and you have to make a decision. There is nothing clean, rinky-dinky, nice and tidy that can be delivered to make it easy for a judge. It is absolutely what judges are not trained to do, as David said. It is exactly the opposite.

I am very happy with the five days. I would be very happy with five-day scrutiny and with the Secretary of State being called in every month to meet the commissioner, who would say, "You made this, that or the other decision", and go over it, but at the critical moment, at 2 or 3 o'clock in the morning, somebody has to make a very difficult decision, and it may be on instinct. In my case, I had been going to Northern Ireland every single week as the Opposition spokesman—as the shadow Secretary—for three years. I had met an awful lot of people, I had been to every corner of Northern Ireland—places where, sadly, I could not even dream of going now—and, in fairness, I learnt a little bit about it. I pulled on that information and on some of the people I had met. David is absolutely right. There is an element of this that is instinct. That is called political judgment. It is not right to put judges in the same box. It is not fair to them.

Suella Fernandes: Where would you draw the line, in striking a balance between national security and transparency in decisions on the issuing of warrants, between judicial and ministerial decision-making power? Would you say that it should be solely for Ministers, with no judicial decision-making power?

Mr Owen Paterson: Yes. I am completely clear. Elected Secretaries of State, accountable to the House of Commons, should make those difficult operational decisions. That will guarantee operational agility and swift reaction. I am all for increasing, extending and making more intense the scrutiny process by distinguished judges, after the event. I mentioned dear old Montesquieu and the separation of powers. It is not a bad thing to go on. He made it absolutely clear that you do not have judges making executive decisions.

Q99 Bishop of Chester: The clauses to which you referred are in Part 5 of the Bill, I think, at the end, on bulk interception warrants.

Mr Owen Paterson: Part 8.

Bishop of Chester: Earlier warrants allow a five-day period when urgent decisions can be taken. Is there a particular reason why you think there should be the facility for an urgent decision, not requiring the judicial approval in the later part you have been referring to?

Mr Owen Paterson: I am very happy with the five days. That could be a sensible compromise. The five days allow decision-making by the elected Secretary of State, without interference, without delay, without obfuscation and without muddle.

The Chairman: Can I stop you for a second to clear things up? The five days refer to urgent cases, not ordinary cases. I think that Mr Paterson is saying that, even in ordinary cases, the five days would become a review, rather than a co-decision.

Mr Owen Paterson: Correct. That is exactly right.

Bishop of Chester: There is the practical question of an urgent request, under the later part of the Bill, for the bulk warrants, but there is not provision for an urgent decision. There is in the earlier part of the Bill. You are raising a more fundamental principle as to whether the judges should not operate as they do now, revealing after the event. You are suggesting that that is much better.

Mr Owen Paterson: The Chairman summarised very effectively what I think. The decision should be made by a democratically elected Minister, accountable to the House of Commons. The review should be conducted by distinguished lawyers, days, if necessary, after the event, with the scrutiny process starting at five days. I would be very happy for Secretaries of State to meet the reviewers more regularly.

Bishop of Chester: I understand that that is how DRIPA, the present time-limited Act, operates. There is judicial review after the event.

Mr Owen Paterson: Yes.

Bishop of Chester: That is what you would prefer.

Mr Owen Paterson: There is no judicial co-decision-making. At the moment, judges do not participate in the decision. Under these proposals—it is called the double lock in all the press releases—they will be very actively involved.

Bishop of Chester: To be quite clear, you are striking, in a sense, at the heart of the principle of what is now proposed.

Mr Owen Paterson: Yes. I strongly disapprove of the proposal that judges make executive decisions.

Bishop of Chester: That is what you are saying.

Mr Owen Paterson: Correct; absolutely.

Lord Strasburger: Could you tell us how many times you were held to account by Parliament? Could you also explain why your views, in particular, are the exact opposite of those of our four "Five Eyes" partners?

Mr Owen Paterson: I do not remember ever being called up before any Committee or having it raised in questions in Parliament. I suppose you could say that that is a tribute to the fact that the system works, in that people were careful before putting requests before me and, I hope, I was also careful in scrupulously reading every detail and not nodding things through. As I said, I did, infrequently, turn them down.

Lord Blunkett: Let us go back. The commissioners reviewed the process and whether we had followed it, within the powers laid down to us, which is what I understand review to be anyway. We also had the annual debate, which, sadly, did not engage the media in the way I had hoped it would. Parliament usually had a robust debate, concentrated mainly not

on Northern Ireland but on the Home Office and the Foreign Office, with some thoughtful contributions, but it was not really holding to account in the sense of people understanding and then asking us to explain what we had done in individual cases, for fairly obvious reasons—we were dealing with sensitive material, which we would not be able to explain. That was one of the Catch-22s about reporting back to Parliament when we were debating Bills, including the one that has a sunset clause next year. How can you report to Parliament on detail that is itself subject to the necessary privacy that protects those who have been involved? That is why your job, and the Home Secretary's job, is so difficult.

I fall slightly short of Owen's absolutism on this. I can see entirely where he is coming from, but in the reality of the moment we have to deal with what has been put forward by the Government and the difficulties that they face. I have to be careful here. My second son works for a major company and years ago used to tell me off for being too gung-ho on all this, so I have family problems. Can I be clear? Whatever the Government decide to do, there are people who do not believe that it is either necessary or acceptable. At the moment, they get a bigger hearing than the intelligence agencies.

The Chairman: Could I clarify something Lord Strasburger said? He made an important point. There is no real parliamentary mechanism currently available, is there, for obvious reasons, that could in any way scrutinise the decisions either of you would make on agreeing intercept warrants—even to the extent, I guess, that the ISC, meeting in private, would not be able to deal with them?

Lord Blunkett: I see no reason why we should not have a much more thoroughgoing report on the number of decisions taken and the nature of those decisions. When the then Foreign Secretary, William Hague, reported to Parliament on the back of what happened with Snowden, I said that we could be a lot less diffident and sheepish about all this, without putting the intelligence and security services and their operatives at risk. We should examine how we might do it more openly. We could also examine areas that are outwith what the Bill is able to deliver, namely where information is provided from other agencies outside this country and there has been no warrant and no clearance. The information is given to us, and we have still not come to terms with that.

Lord Strasburger: You seem to be confirming the view that the concept of parliamentary scrutiny of warrants is a myth.

Lord Blunkett: I do not know anyone who has really believed that Parliament scrutinises the warrants system.

Lord Strasburger: Exactly.

Lord Blunkett: The commissioners have. They produce their annual reports, which are usually commented on in the media, but Parliament, other than in the annual debate, does not and has not.

Lord Strasburger: But both of you gentlemen, particularly Mr Paterson, have waxed lyrical about the concept of parliamentary scrutiny. I am struggling to see where it is.

Lord Blunkett: No. The politician is accountable. That is different from the way in which Parliament chooses to scrutinise or not to scrutinise. Secretaries of State are accountable, both publicly and to Parliament, and can be sacked. I wonder under what conditions a judiciary involvement would result in their being removed.

Mr Owen Paterson: That is the key point: we are accountable. There is a lot of information about decisions made by Secretaries of State. Ultimately, those decisions can be taken up by parliamentarians, should they choose to do so. As David said, at the moment there is only a debate. Should things go wrong, Secretaries of State can absolutely be on the line and accountable to Parliament.

Lord Strasburger: As far as I know, it is not legal for a Secretary of State to discuss a warrant in public.

Mr Owen Paterson: But a Secretary of State is accountable to Parliament for activities in his or her sphere of influence—and can be fired.

Victoria Atkins: I can help Lord Strasburger. Sections 17 to 19 of RIPA make it a criminal offence for Secretaries of State to answer questions on this, if they are so asked. That may help to answer his question.

The Chairman: You have been let off the hook today.

Lord Blunkett: That never passed across my consciousness when I was there.

The Chairman: I move now to Lord Henley, because Mr Warman's questions have been answered.

Q100 Lord Henley: I want to come on to the various safeguards for privileged communications. You will remember the statement that was made by the Home Secretary on 4 November and the concerns raised by David Davis, in particular, about the lack of protection that MPs have over the potential acquisition of their communications data. Does the enshrining of the Wilson doctrine in statute provide adequate protection for legislators' communications and address the concerns put forward by David Davis, or should there be additional safeguards over the use of communications data for parliamentarians, as there are for journalists?

Lord Blunkett: It may be worth cross-referencing briefly to the inquiry that took place after the incursion into the Palace of Westminster in the Damian Green affair. That was old-fashioned taking away of materials, as opposed to intercepting them through new, modern information, communications and Internet provisions, but the principles were the same. That Committee, on which I served, was under the chairmanship of Ming Campbell, now Lord Campbell. It is worth testing it out. If we are honest about it, the Wilson doctrine was more in intention than it was in reality. How carefully can I put this? What you are doing in this improved Bill is what we were trying to do. My predecessor, Jack Straw, brought in RIPA, and I had the undoubted "privilege" of implementing it. The intention was to be helpful, although people have interpreted it entirely differently since. On the Wilson doctrine, we should distinguish what is privilege in terms of protecting

Owen Paterson's electors—my previous electors—from the issue of protecting the parliamentarian. Over to you, Owen.

Mr Owen Paterson: That is a good way of putting it. The principle of privilege, not the individual, is the key point. My main concerns with the Bill are to do with warrantry and powers of decision-making. When it came out, I read it and saw the statement that any proposal involving an MP or any other elected body—the Scottish Parliament, Welsh Assembly et cetera—has to go to the Prime Minister. There has to be an element of common sense. To go back to Suella Fernandes's question, it is a bit of instinct; anyone who thinks of putting any marker down on an MP has to think really carefully in advance. Common sense will probably be the best defence.

The Chairman: That was another very interesting, riveting session. We are very grateful to you both, because it has come from a totally different perspective from that of our earlier witnesses and gives another interesting aspect to our deliberations. No one can say that both of you have not put your views with great robustness. Thank you very much for coming along.