HOUSES OF PARLIAMENT

Joint Committee on the Draft Investigatory Powers Bill

Oral evidence: Draft Investigatory Powers Bill, HC 651

Wednesday 9 December 2015

Watch the meeting

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

Questions 101-136

Witnesses: Mark Hughes, President, BT Security, **Adam Kinsley**, Director of Policy and Public Affairs, Sky, and **Hugh Woolford**, Director of Operations, Virgin Media

Q101 The Chairman: A warm welcome to the three of you. Thank you so much for coming along. You represent very significant companies with a lot of relevance for this particular Bill. Apologies to you for starting a bit later, but there was a vote in the House of Commons, which delayed our procedure. I am going to kick off the questions by asking you all to answer the one I am going to ask. If you want to say anything by way of a short general statement, perhaps you would like the opportunity so to do when I have asked the question. Again, welcome to you.

My question is a fairly simple one: how extensively is the Home Office engaged with you with respect to the provisions in the Bill? Perhaps Mr Hughes would start.

> ***Mark Hughes***: We have been consulted. We welcome the consultation that we have had. We have had a number of opportunities, and, overall, we are pleased with the level of consultation. There are obviously circumstances where it could be better and we could have done more, but, broadly speaking, it is very different from previous iterations we have had with the Home Office so we are comfortable with the consultation that we have had.

The Chairman: Thank you very much. Mr Kinsley.

> ***Adam Kinsley***: Indeed. I would echo that. There has been extensive consultation over the last months and it has been a marked improvement on last time.

The Chairman: Good. Finally, Mr Woolford.

Hugh Woolford: I would echo that. We have had engagement, and we have had high-level engagement both on the legal and operational sides. It is welcome that we are having that engagement.

The Chairman: That is a good start. Lord Butler.

Q102 Lord Butler of Brockwell: Following on from that, you are satisfied with the consultation, but has it led to agreement about what is practicable? Let me elaborate on that while you are thinking about it. This is on the nitty-gritty of how it is done. I am after whether you think it is practicable to separate communications data from content, or at least the type of communications data you are being asked to retain, whether you are confident that you have the equipment that would enable you to do that, and whether you can give us some idea of what degree of extra costs that would impose on you. I hope that is not too much of a question.

Hugh Woolford: I will kick off and then pass across to my colleagues. I will take it in bits. On how easy it is to separate communications data from content, in the dealings we have had to date we feel that we need more work to get more clarity over what is considered content versus communications data. We need more workshops between the bodies to flesh that out. At the moment there are very high level—

Lord Butler of Brockwell: Excuse me, but does "bodies" mean the Home Office and the providers?

Hugh Woolford: Absolutely, yes. At the moment there are very high-level definitions. You could, for example, say that a route URL for bbc.co.uk is considered communications data, but if you put a "/news" on the end that may be content, so there are nuances—this is the way the Internet is constructed and used—that mean that does not always hold true. There are some general principles in place. We need to move forward and get some more detail in place around some of those nuances and how to handle some of them. That is the first point.

Leading on from that, given that we have not got to the nub of how we would differentiate, the answer is no, to be perfectly honest. We have early discussions going on with regard to some of the equipment or angles that we could look at, but there is a huge piece on volumes, which I am sure we will come to later in the session, that has a massive bearing on the equipment that we need and therefore also the cost.

Adam Kinsley: At this stage, we have to differentiate the conversations and the factsheets we have seen and what we are looking at in the draft Bill. The draft Bill is obviously very high level and it is not sufficient to be able to map across from that and understand exactly what we are going to need to do. By definition, it is going to have to come later in codes of practice and in further discussions. Going back to your question, to be able to differentiate and look at communications data within what are effectively packets of data, there will need to be investment in new types of technology for us to be able to get up to the first slash. The way the Internet is arranged and operated is not simple. We are going to have to look at individual use cases and understand exactly what we will need to do. Hopefully, that answers your question.

Mark Hughes: There are a number of parts to the question. The first is whether or not it is technically feasible to separate content from communications data. The draft Bill usefully defines communications data both from an entity and an event point of view, which is a new set of definitions, as opposed to the previous or existing regime—the RIPA regime—and then content. Technically, it is feasible to separate various parts of the packets; we can deploy tools to do that. The point about that is that, increasingly, especially in the future, with more and more encryption, the ability becomes more limited to take you back to purely an entity level piece of communications data as opposed to richer parts of communication data. That is the first thing.

More broadly, there is a lot of discussion, and has been, about definitions. We have already started talking about them today. It is important to look at definitions in the context of the level of intrusiveness that is the purpose behind the power being sought. That is always the reference point. The definition comes from the level of intrusiveness that is going to impact on our customers and on citizens generally. The definitions are derived from the level of intrusiveness to help bucket, effectively, certain types of data, be it first slash-type data or whatever it may be, to have a way of defining certain types of data. The caution I always put on definitions is that it is not easy to write them down, and we can see that right across the Bill, but with the additional checks and balances put into the draft Bill around legal oversight stuff, there is the possibility to refer back to the level of intrusiveness. Where the definition in the draft Bill might not be sufficient at the moment, there is the possibility through oversight to question that.

I think your next point was about whether or not the equipment exists. Yes, it does. There are various technologies available to us, although they are limited by the way in which the traffic is sampled, and there are many considerations around that. Indeed, some of the Bill, especially in the area of Internet connection records, which are new data that we have never collected before for that purpose, means that we will have to deploy new equipment to comply with the legislation as it is drafted. That comes at a cost. Clearly, there are two things about costs that concern us. First, it is not clear in the Bill at the moment that we will be eligible to recover all our costs, and we think that is important for two reasons. First, the mere fact of defining how much something will cost to meet a certain type of power will help to limit and frame the level of intrusiveness. In other words, an open-ended view of what something could cost could be problematic in the sense that capability could be stood up, which could cost a lot. Therefore, a proportionality check comes in through ensuring that it is clear that costs will have to be met. Secondly, clearly, if the cost is not met in that way, it will have to be found in some other way. There will be additional costs and we certainly have some views on some of the calculations—perhaps we might talk about that later on.

Lord Butler of Brockwell: When agreement on definition is reached, how do you envisage that it will be expressed in statutory form, or would it be expressed in statutory form? Would it be by a statutory instrument or will further amendments to the Bill be necessary?

Mark Hughes: This process, through scrutiny, is in part helping to tidy it up. There is, I believe, much more work to be done to ensure that we get tighter definitions where we can. Equally, as in my previous point, we have to ensure that the oversight regime allows us the ability to discuss that. More specifically, to answer your question, the codes of

practice, which we look to see before the publication of the final Bill, will go some way to clarifying a lot, as well as the oversight instruments that exist in the draft legislation, which will allow us, if we are not comfortable with that, to visit it with the appropriate authority.

Q103 Lord Strasburger: Gentlemen, you have mentioned encryption as being a complicating factor. We have also heard in previous sessions that the way the Internet is increasingly being used—for example, with a Facebook page—is as a smorgasbord of content and data, and that it may be impossible to separate them automatically. I doubt that you would fancy doing it manually. How are you going to cope with that problem?

Adam Kinsley: You have put your finger on the nub of the technology challenge. When you are requesting a page within Facebook, facebook.com/spurs, or something like that, you are going to get lots of different content delivered: you are going to get the league table, the Harry Kane goal or something like that—lots of data. We need technology to analyse all of that, match it all up and work out which bit is the first slash. It is a big technology challenge. As Mark says, it is not impossible but it is very expensive.

Lord Strasburger: Thank you.

Q104 Dr Andrew Murrison: Obviously, there is some urgency to all this because the Home Office would rather like to get cracking with gathering the information that it says is necessary to safeguard security and deal with serious crime. I am interested to know from you how long you think it is going to take, given the technological challenges that you pose, to get to that first slash point.

Hugh Woolford: We have put some thought into the timescales. As long as the necessary discussions and detail were worked through, we feel that we could probably start in 2017, with earliest deployments in 2018, depending on the requests and the scale. Those are the sorts of timescales that we would potentially be working to.

Dr Andrew Murrison: That sounds quite a long timeframe to me. Does that match the level of patience that you perceive in your dealings with the Home Office, or is it disappointed by that?

Hugh Woolford: I honestly cannot comment on that. Those are the timescales that we have in mind. That is currently where our heads are.

Dr Andrew Murrison: I have to say that the definitions on the face of the Bill confuse me; I suspect that they will probably be rather clearer to you since you are in this particular business. I have heard from you already that you value the improved definitions, particularly those in Clause 193, which I guess is what you are referring to when talking about entity data and events data, but I am also hearing that you expect further clarification by way of codes of practice. Where do you think we are at the moment with the definitions? Where on a Likert scale of zero to 10—where zero is completely useless and 10 is perfection—do you think we are at the moment?

Adam Kinsley: I am not sure that the intention is for us to be able to deliver any capability based on the face of the Bill alone. As it stands, it is pretty close to zero, I would say. We

absolutely need more detail to be able to deliver. I am not sure it was the Home Office's intention to be able to deliver based on the definitions on the face of the Bill, but that is obviously a decision for Parliament—how much goes on the face of the Bill, how much goes into codes of conduct.

Mark Hughes: There has been a lot of work to help to clarify a number of the definitions in the Bill. In the Internet connection records space, for example, it is difficult for us to comment because we are not defining the purpose for which it is intended. Therefore, by its very nature, I am not in a position to comment. There has been a lot of work. As we have already said, there needs to be more work and the codes of practice should support that.

Adam Kinsley: I should qualify my comments. I was answering in relation to Internet connection records primarily.
Hugh Woolford: I would echo that.

Q105 Mr David Hanson: Page 25 of the draft Bill, regarding Internet connection records, says helpfully: "A kind of communications data, an ICR is a record of the Internet services a specific devices has connected to, such as a website or an instant messaging application. It is captured by the company providing access to the Internet". Is that your understanding of what an Internet connection record is?

Hugh Woolford: Today we do not have anything like an Internet connection record. This is something that is completely new for us, and I have looked at previous Bills. From a business point of view, there is no need for us to capture any of this information. We do not have what could be classed as an Internet connection record.

Mr David Hanson: I am a layman here, so tell me how hard it is to collect one of those, to establish it.

Mark Hughes: On the face of it, it sounds like a relatively straightforward thing to do. In some respects, the Bill goes on to define the purposes for which they are being collected, and three purposes are outlined. They are obviously around the person, illegal content and the service, broadly speaking. It helps as well when you combine the two things; you take the initial definition and the purposes that are in the draft Bill, and that has given us a route to analyse what would need to be collected—as Hugh said, it is not something that we collect today—to fulfil that definition and then have data available if that were to be the case for that purpose. You would have to look at quite a lot of data to be able to achieve that.

Adam Kinsley: If you think about what a CSP would be required to retain at the moment, essentially you may be given an IP address that would be applicable to your computer for potentially up to a week and that would get recorded once. There are a couple of bits of data that would be recorded for about a week. In what the Bill is seeking to do, first of all you would have to analyse all your Internet sessions in that week—in fact, throughout the whole year—which would obviously be quite a lot; in the Facebook example we used earlier, just one request to a Facebook page will come back with lots of information within it that needs to be matched. You need to analyse all that, match it all up and then retain the

bit that the Bill will ultimately end up with. The magnitude of data collected that would be processed would be massively more and the magnitude of data that would then be retained would be tenfold, a hundredfold more than we collect today.

Q106 Mr David Hanson: At the moment we are considering the draft Bill; it is going to go through the House of Commons and the House of Lords and be law by September or October next year. How long is it going to take you to establish the mechanisms? How much is it going to cost you to establish the mechanisms? Who do you think is going to pay for this? Is it the taxpayer, as in all of us? Is it you or a mixture of both? If so, what is the mixture? Is it practicable? Is it going to do what it says on the tin? We need to get a flavour of this from you.

Mark Hughes: Let me go through a number of those things. There is a spectrum of options available on Internet connection records in terms of the amount of coverage. The Home Office has consulted us and we have had a pamphlet that has been issued about Internet connection records, with some view of costings. We have obviously done work based on the assumptions. The assumptions from the Home Office are that it wants as broad a coverage as possible to achieve this, which is going to be costly. We have worked up some assumptions and indicative costing.

Mr David Hanson: Are you able to share that with us or not?

Mark Hughes: Yes. The publicly stated figure, I think, from the Home Office is that it has set aside £174 million for this. We have worked out that for us alone—I cannot comment for others around the table or others in the industry—to fulfil the assumptions that we have been given will cost us tens of millions, so the lion's share of that £174 million would be for us alone. How others would do it depends on how they manage and architect their networks. We have looked at it. As to the implementation time that it would take, again it depends: there are some things where extant capability could be used to gain some coverage relatively quickly, but to fulfil the assumptions we have been in dialogue with the Home Office on, it would take longer to deploy equipment comprehensively across our network—deep packet inspection equipment—to be able to generate the data to then have them retained to comply with the legislation.

Hugh Woolford: On costs, we broadly agree. Our teams have had a look at the high-level information we have and think similarly—tens of millions. I would love to give you an exact figure. We are not saying it cannot be done. Anything can be done in this space with enough time and money. We have a broad set of requirements, but to enable us to move forward we need to bring some more specificity to those so that we can start giving more accurate estimations of costs and time. Depending on how much you are trying to capture and across what frequency, one big piece of it is how much of whatever the equipment is you might need to deploy; therefore, you need to find space, power and places to host it all. It is no mean feat. This Bill potentially could look at all of us having almost to mirror our entire network's traffic to enable us to filter it. It is a huge undertaking.

Mark Hughes: You asked about costs. We believe quite strongly that the costs should be met by the Home Office—that we should seek to have 100% of our costs in this space reimbursed. The reason is that, if you start from the basis that there is no cap on the cost,

you may end up with a disproportionate technical solution that could be overintrusive, so the cost in itself will help bound the solutions.

Mr David Hanson: To help the laymen and women among us, if the taxpayer chose to support the cost of developing this scheme, do you think £170 million is a reasonable estimate, given what you have said in your previous answers, or not?

Mark Hughes: Based upon the assumptions we have seen, from our point of view, yes, because it would cover what we need to do, but if you aggregate it across the industry—

Mr David Hanson: It is not just you, is it?

Mark Hughes: Absolutely not.

Mr David Hanson: Otherwise the terrorists and criminals would not use BT; they would be using something else, would they not? So it cannot just be you.

Mark Hughes: Indeed. There are obviously other ways in which other networks are architected. There are, though, other assumptions. You could use less sampling of traffic, which would perhaps give less coverage, but there would be a trade-off in the amount of cost.

Q107 Mr David Hanson: This is the final question from me, Lord Chairman. Let us look two or three years ahead to when this has all been done, someone has paid for it, it is all available and the aspirations on page 25—of the Government and you—have been met. What do you think about how the Government access that material? Are there sufficient safeguards in the Bill for single point of contact officers? Are there sufficient safeguards in the Bill for access by the security and police forces via the Home Secretary, or whoever, in the Bill?

Mark Hughes: On that point, the Bill is clear that there are three purposes under which the data we are talking about, the Internet connection records, can be disclosed. That is fine. However, there are further parts of the Bill that refer to forward-looking capability. We believe, going back to one of the points I made earlier, that that potentially changes the intrusiveness before the data are disclosed and would, in our view, require a check against the level of intrusiveness that it would incur and a referral back to the legal oversight to ensure that we were not stepping outside the intention that was originally conceived in the three purposes.

Hugh Woolford: Can I raise an item on the emergency single point of contact? One of the items that is suggested is emergency SPOCs. We feel that could give rise to an ability to breach the system. In an hour of need—the golden hour—how are you going to validate who is asking for the information? It would be better if the normal SPOCs—if "normal" is the right word—were to provide cover so that there was a single list of authorised people who can ask for it. Having an emergency, somebody ringing up or contacting and saying, "We need this because someone's life is in danger", gives an opportunity for that to be abused. We feel it is better if the SPOCs cover each other. That is an area that we would like to have looked at.

Mr David Hanson: Apart from that, it is all going well.

Q108 Stuart C McDonald: I have one short supplementary on these points. One or two witnesses made reference to a similar scheme that was operated in Denmark. Is that something you guys have looked at? What were the similarities and differences? Is there anything that can be learnt from what happened there?

Hugh Woolford: No, I have not looked at that, I am afraid.

Mark Hughes: I understand that the system in Denmark has failed because the software has not worked. That is what I am led to believe.

Stuart C McDonald: Is there anything we can learn from that? Is the scheme that you are being asked to implement similar?

Mark Hughes: I am not familiar with the ins and outs of the detail of it; I am just aware of the headline. Through the consultation and the technical feasibility that we have done, we believe there are technical solutions that we can put in place—subject to the Technical Advisory Board confirming that. They would perhaps draw on that Danish experience, but we have to be careful that we implement them properly. There is no reason why, if we have the right solution and we implement it properly, it will not work.

Q109 Lord Butler of Brockwell: I have one supplementary. Could you break down the £174 million between the one-off cost of getting the right equipment and then the recurrent cost of maintaining it?

Mark Hughes: The capital investment—the deep packet inspection-type equipment that needs to be put in place—has to be factored against the very strong growth, or fast growth, in bandwidth over the period. The Home Office looked at this over 10 years. Then there is obviously the ongoing cost of maintenance, but also primarily storage. There is an initial upfront investment, but storage is the thing that is going to take up a fairly big chunk of that cost.

Lord Butler of Brockwell: Can you give us an indication of how much of the figure you gave is the once-and-for-all cost?

Mark Hughes: I do not have the figures off the top of my head, but it is skewed quite heavily towards making sure that there is storage. It is not to say that the initial investment is not insignificant, but the storage is also a significant part of it.

Lord Butler of Brockwell: We are talking about £174 million per year, are we?

Mark Hughes: No. From my own point of view—BT's point of view—it is a fraction, so to speak, of that, but we look at it over a time period. There is an initial upfront investment and thereafter the storage.

Adam Kinsley: It is possibly worth adding that, whereas in the previous regime data growth did not matter that much, in this regime it very much would and data growth is running at doubling every 18 months or so. That needs to be factored into any equation.

Q110 Suella Fernandes: It will be a challenge to maintain the security, but to assess the challenge that is going to be presented by the Bill, what in a technical capacity is available to you to reassure the public on the security of data retention?

Hugh Woolford: We have discussed this. We will obviously look to work with the government security advisers to ensure that any processes and systems that we put in place to meet this Bill would meet those requirements and then regular auditing of them. That is the best way we think we could assure that everything was secure and in place. As a matter of course, you have to create a culture and a process around it that brings rigour.

Suella Fernandes: What is your assessment of the effectiveness of things like firewalls and personal vetting systems, and how realistic are they as tools to expand on?

Mark Hughes: It is about creating a layered approach to defence, ensuring that the controls are proportionate, given the sensitivity of the data. We are talking about collecting data for the first time—data we have not collected before—and the key is to ensure that our customers and their rights are protected. That data has to be looked after very carefully, so we have to have a commensurate security wrap around them that takes account of our customers' human rights and indeed their privacy as well so that we ensure that we maintain and safeguard that.

Adam Kinsley: We currently work with the Government on standards, but it could benefit from being more joined up on the Government's side. The Home Office, the ICO and the National Technical Assistance Centre having a single set of standards that we could build to would make a lot of sense.

Mark Hughes: We see a key role for the proposed Investigatory Powers Commissioner and its office being responsible. Clearly the Information Commissioner's Office has a role as well, but it would be useful to us in this context to have a joint agreement between the Investigatory Powers Commissioner and the Information Commissioner's Office, perhaps through a memorandum of understanding. We would rather have the Investigatory Powers Commissioner as the authority to which we could go to seek advice to ensure that we were meeting the correct standards to safeguard that information.

Suella Fernandes: Of course the Information Commissioner will have an auditing power over the security of the systems. How would you describe the appropriate level of engagement with the Information Commissioner?

Adam Kinsley: In the past we obviously had normal business interaction with the Information Commissioner. It seems to us that with this opportunity, when we are creating a new commissioner for these purposes, it might make more sense to bring all of that under one roof; if we are looking at the security of these specific systems, now might be the time to look at having it all under the Investigatory Powers Commissioner rather than two separate organisations.

Hugh Woolford: We absolutely echo that. It brings clarity and conciseness. That is our absolute view. We would rather have it brought under one, definitely.

Q111 Suella Fernandes: This is my last question. There is some suggestion of introducing a criminal offence for data breach by communication service providers. Do you think that is going too far? Do you think it could act as an incentive?

Mark Hughes: We take the privacy and security of our customers' data extremely seriously. As is well reported in many parts of the press, it is something that we take so seriously that we do not necessarily see criminal powers as necessary. We already take it extremely seriously and we believe that the sanction if something goes wrong is that one can quite clearly see the consequences almost on a daily basis.

Hugh Woolford: That is more or less what I was going to say.

Q112 Stuart C McDonald: I want to ask about request filters. What is your understanding of how a request filter would work, and what concerns, if any, do you have regarding its operation?

Hugh Woolford: We have had engagement on the request filter. It is not specified as such in the draft of the Bill. We understand that information would be asked for, we would pass it into a filter and then ensure that only the specific information is passed back, so it stops massive information coming back. We have a few specifics, but the principle is purely at high level, as a concept more than anything else, at the moment. Without wishing to sound like a broken record, this is something else that definitely needs to be looked at and worked through in more detail. One thing that we do not want to do is to become data analysers of information.

Mark Hughes: We understand that it is for the Home Office to design and build the request filter and that it will sit between us as a communication service provider and the law enforcement agency. That is how we see that it will work, but, as Hugh said, there is more to be done. It will use an algorithm essentially to limit the data that are disclosed or presented to the law enforcement officer, who is obviously authorised to see the data, so it limits the data just to those who are necessary to that question.

Stuart C McDonald: Does the information you have just given arise from discussions you have had with the Home Office?

Mark Hughes: It is what I understand from discussions we have had with the Home Office. We have a concern, once the system is effective and in place, that there could be a situation where lots of questions are asked and continue to be asked of it, so our view is that more work needs to be done through consultation to ensure that we—again, going back to my previous point about intrusiveness—level up if multiple questions lead to a point where it is becoming overintrusive. An important principle for us throughout the Bill is that we should always level up to the highest level of authority when we think intrusiveness is becoming greater than was originally intended.

Lord Strasburger: There is a view abroad that the provision in the draft Bill for the request filter is not much more than a placeholder for the Home Office to return to this in the fullness of time and, effectively, write its own cheque on what this will deliver. From what you are saying, it is not giving you very much detail about what this is to do. Is that a possibility?

Adam Kinsley: I would not like to comment on whether it is a possibility. As I understand it, the request filter is there to limit and to be a protection against the flows of information. I would not want to speculate where it might go. We certainly have not seen—

Lord Strasburger: The fact is we do not know where it is going.

Adam Kinsley: The fact is we have read factsheets and had discussions about the concept.

Mark Hughes: The thrust of it is that it is about limiting the amount of data that will ultimately be disclosed to answer a particular question, which is important from a proportionality point of view.

Q113 Lord Henley: Can I turn to the maintenance of technical capability and what is proposed in Clause 189 of the Bill, which you will be aware of? As you know, the Secretary of State will be able to impose various obligations on relevant operators and that will take the form of a technical capability notice, and she will obviously have to consult about that. What are your views on the ability of the Secretary of State to impose a technical capability notice? How do you think your customers are going to react if they are aware that the power exists but they will not be aware of any specific imposition, because that will not be disclosed?

Mark Hughes: There are a few points on technical capability notices. The first one is that we believe quite strongly that the Bill should be clearer in its definition of the fact that the capability notice should be limited to public telecommunications services. At the moment, the definition is not clear, and we are quite clear that it should not extend to private services; it should be limited specifically to public telecommunications services. The second point is that the notice should be served on the provider who is closest to where the information can be provided from. You used the example of Facebook earlier on. That is a matter for Facebook to deal with and the technical capability notice should be directed at that organisation, if indeed it is the closest to the information, which is its information. It should be served, therefore, on those closest to the place where the information is maintained. Beyond that, the existence of a technical capability notice, as in the draft Bill, formulated through the Technical Advisory Board, is good. That there is consultation and oversight that needs to happen before it can be issued is a positive thing.

Lord Henley: What about the views of your customers?

Hugh Woolford: It is definitely not my place to comment on what the views of our customers may or may not be, I am afraid. We are concerned about that, absolutely, but at the moment we have not consulted with them or asked them, so it is wrong for me to offer up an opinion.

Mark Hughes: It is not the technical capability notice per se; in entirety, all the notices that come from this, those beyond the technical capability notices, are something that our customers need to be aware of. Transparency is one of the reasons for this new Bill.

Q114 Lord Henley: You mentioned oversight and the importance of that, and it was partly dealt with in earlier questions from Ms Fernandes about the Information Commissioner. I forget who answered this and whether it is your collective view, but I got the impression that

you would like the proposed Investigatory Powers Commissioner and the Information Commissioner to be one—to be merged.

Hugh Woolford: Yes.

Mark Hughes: I am not advocating a merger, but for the purposes of the Bill we feel that for the Investigatory Powers Commissioner there should perhaps be some memorandum of understanding with the Information Commissioner. As I understand it, the Information Commissioner has many other jobs to do beyond this. There is no merging of the two, but just for the purposes of this Bill it would be useful to have one place to go to. We are all agreed that it is the Investigatory Powers Commissioner.

Lord Henley: Because the Information Commissioner is doing other things, in other words, he would delegate his bit of it.

Adam Kinsley: I am not sure how you would bring it into effect. If what we are talking about is security oversight of systems designed to fulfil the obligations in the Bill, it seems that the specialist commissioner would be best placed to carry out that function.

Mark Hughes: Can I make one more point about the technical capability notice? Following on from the point about those providing the service, and that the one closest to the service should be the focus of the Bill or any action that is served, it is not appropriate, we believe, for a network provider to be used as a one-stop shop. It is absolutely important that we process and manage data on behalf of our customers. Where that data is processed by another organisation, it should be subject to the technical capability notices.

Hugh Woolford: Adding to that, if I may, the retention and storage of third-party data is something we are also concerned about, linked with that whole piece. We do not want to be seen as that one-stop shop and asked to retain and store data for third parties that are not to do with our core business or core customer groups.

Lord Strasburger: How do you feel about GCHQ engaging in covert bulk network interference against your networks?

Adam Kinsley: I personally do not have a view on that. That is a matter for you guys to consider.

Q115 Lord Strasburger: My question is: how do you feel about your networks being amended covertly by GCHQ and the risks associated with that?

Mark Hughes: It is important to note that any power in the Bill that is instigated in that particular arena has to be proportionate and has to have the right checks and balances over the amount of intrusiveness. The oversight has to take account of the fact that, by their very nature, those types of powers are quite intrusive, so the levelling-up process of the oversight needs to be such that there is full legal oversight.

Lord Strasburger: My question was about the risk to your networks. That is what I was asking about.

Mark Hughes: We are certainly not in favour of anything that would undermine the integrity of our networks.

The Chairman: Gentlemen, we are very grateful to all three of you. Thank you very much for coming along and giving evidence to us.

Witnesses: James Blessing, ISPA Chair and CTO of Keycom, and **Adrian Kennard**, Managing Director, Andrews & Arnold Ltd

Q116 The Chairman: Welcome and thank you for coming along to give evidence to us on a Bill which is extremely important for the country and for organisations and companies like yours. I am going to ask you a fairly straightforward question to begin with, but if in answering it you want to make a general statement, please feel free to do so. How extensively has the Home Office engaged with you with respect to the provisions contained in the Bill?

Adrian Kennard: Not at all really. As a small ISP, the only involvement we have had is that ISPA—the Internet Service Providers Association—was invited to a briefing after the Bill was published to try to explain it to us. That is the only involvement we have had.
James Blessing: As ISPA we tried to engage beforehand. We made representations. There was not a long dialogue until after the Bill was presented. It has been a bit difficult on that side of things. As a service provider—I do both—there has been no conversation whatsoever.

The Chairman: It is perhaps important to explain to the Committee that Mr Blessing acts in two capacities, with his own company but also as chair of ISPA.

Q117 Lord Butler of Brockwell: In the absence of discussions with the Home Office, to the extent that you have been able to think about what is proposed by way of separating communications data from content, have you any view about whether it is practicable?

James Blessing: It is practicable as in it can be done. It is not practicable in many senses because it is not clear what is required to be done. Because the Bill does not on the face of it say exactly what is required to happen—what information is required to be captured, what format it is to be stored in and how it is to be made available—it is very difficult to design a solution that works and does all the things it needs to do, which is secure, safe and retains the data needed by law enforcement to continue its investigations. Part of the issue is that the Internet connection records do not exist. They are not a thing. They are not generated in normal business. We do not have them. They are a new thing that has been created, and because they are not defined it is difficult to say how you would go about creating them.

Adrian Kennard: I have concerns about the definitions as well. The communications data depend hugely on the context of the communication. The definitions make something like a phone number communications data, but that should only make sense in the context of a telephone call. If it is buried inside an email, is it still communications data? It seems that the Bill could consider it that, and could give the Home Secretary power to have a snoop on the content of information to pull out anything that is an identifier, like an email

address, a phone number or someone arranging a meeting. It is quite important that the definitions relate to the context of the individual communication.

Lord Butler of Brockwell: Where do you expect that definition to be made? Are you expecting it to be made in the code of practice—clearly there will be further work—and how long do you think it will take?

James Blessing: In an ideal world we would like it in the Bill itself. Having what is required clear and transparent in the Bill makes it easy for everyone to understand what is being collected. The Internet industry is slightly different from many other industries in the fact that we depend on each other to be able to do what we do. Therefore, we tend to discuss in open forums solutions to problems that we commonly have. If collecting Internet connection records became a thing and it was clearly defined—"This is what they are"—it would be something we would sit down in rooms and discuss and for which we could come up with solutions that worked for us. Our networks are all very different. They are all designed, grow organically over time, and change and adapt depending on the types of customers we have, so there is no single solution that will work for everybody. Even with two networks that look very similar, their solutions will not work, because they will have some exceptions that cause a problem. Unless that is clearly codified in the Bill itself, it makes trying to work out what is going to happen very difficult. The code of practice has not been published. Even a draft version of the code of practice has not been published, which again leads to the problem that there has been no scrutiny, no review of it. From my understanding, the Internet connection records are going to be defined in individual orders from the Home Secretary, which leads to another problem in that we cannot discuss them with each other. There may be operational reasons—we do not know—but the problem is that we have no visibility and no way of talking about them because we are prevented from discussing them with any other party.

Adrian Kennard: It is worth pointing out that the previous regulations provided a very specific, clear menu on the face of the regulation as to what could be retained—telephone numbers for telephone calls, text messages and email addresses. It would be massively helpful if the Bill spelt out exactly what data need to be recorded; what there is currently an operational justification for retaining should be spelt out in the Bill. That would help massively with these discussions, because we would be able to understand what we might be asked to record.

Lord Butler of Brockwell: Would it not be a little inflexible to put it in the Bill, because as technology changes and the world goes on, you would need amendments? Would it be sensible for it to be in a statutory instrument so that it is there in public and everybody can see it?

James Blessing: It would, as long as it is some form of document that is published so that we can all see it and discuss it. Statutory instruments would work as well, as long as they can be discussed in public.

Adrian Kennard: If that is to be the case, it is important that what the initial SI will be is available when the Bill is considered by Parliament, because what data needs to be recorded has a massive impact on costs. I know technology changes over time, but I am

not sure that granting the Secretary of State such wide powers with those very vague terms is justified simply in the name of future-proofing. It does not usually work.

Lord Butler of Brockwell: Directions from the Home Secretary are unsatisfactory because they are confidential. Is that the point you are making?

Adrian Kennard: That is important.

James Blessing: It is important.

Q118 Dr Andrew Murrison: I do not have much more to ask on this particular bit, Chairman, except to say that the definitions are rather refined in this piece of legislation compared with its predecessor legislations, which in part this is meant to replace. I am getting from you that we have a long way to go yet for this to be in any way a workable document, and that you would prefer to see the codes of practice or statutory instruments published at pretty much the same time as the Bill, since without those the Bill is pretty pointless, is it not?

James Blessing: Yes.

Dr Andrew Murrison: Is that it, in a nutshell?

Adrian Kennard: Yes, I think so. You say they are more refined. The previous regulations were very clear—telephone numbers, email addresses. This is about identifiers that could refer to equipment somewhere in very vague terms.

Dr Andrew Murrison: Forgive me, I was thinking more about electronic data than about telecommunications—telephone—data, which I accept are much easier to record and are recordable in any event for billing purposes. This is in a different space entirely, is it not?

Adrian Kennard: Yes. I am sure ISPA and telecommunications operators would be happy to work on coming up with some clear definitions to help you, to specify in clear terms what an Internet protocol address is and what an email address is, to give you an idea of what those data are and how they could be written down.

Dr Andrew Murrison: I am slightly disappointed that the Home Office has not already done so, because we are presented with this whopping great draft Bill, yet we are pretty unclear about the definitions; indeed, when questioning your predecessors on the panel and asking them to put it on a Likert scale of zero to 10, where zero is rubbish and 10 is extremely good, they said it was zero, which is a cause for concern.

Adrian Kennard: That sounds a bit negative.

James Blessing: There are some nice bits in the Bill that clarify a few things in a nice way. They are a rare beast within the Bill as a whole.

Adrian Kennard: I get the impression that the Home Office has spoken to the larger ISPs. It said as much in the meeting we had. In order to come up with the cost estimates it must have a clear idea what information it is asking for. While we would love to help specify

the data that can be collected so that that can be put in the Bill, the Home Office has just left it out. I do not think it is that it does not know. It must have an idea to get the costing.

Dr Andrew Murrison: It is simply relying on putting it in a supplementary piece of legislation.

James Blessing: Or not putting it in any legislation whatsoever and just doing it as part of the notice from the Home Office.

Adrian Kennard: I think that is what it wants to do.

Q119 Suella Fernandes: When it comes to the issuing of retention notices, you understand that there will be an assessment whereby the Home Office is not going to issue them on all service providers. It takes into account the costs, the feasibility and the volume, and that is going to be informed by the Technical Advisory Board. There is a heavy element of discretion and consideration as to the practical implications. You appreciate that, do you not?

James Blessing: We appreciate that very much and it is the correct approach. The problem is that operational needs change, and the requirement for an ISP suddenly to get a notice because its particular group of customers is of interest to law enforcement means that we all, as service providers, have vaguely to sketch out how we would do that. When it is a nebulous "We are not quite sure what we are doing", you can do that, but you cannot plan to say, "I will make these changes to my network should I get that notice". As part of the Bill, we have gone from a situation where cost recovery was quite clearly stated as, "It is definite that you will get your cost recovery", to a slightly woollier version, which says that the Home Office "may" provide some cost recovery.

Suella Fernandes: But it is clear there is the duty to consult. It is very much a two-way process.

James Blessing: Yes.

Suella Fernandes: Lastly, there is also a power for you to appeal, whereby if it is disproportionate, whether on a practical or cost basis, the decision can be reviewed.

James Blessing: Again, that is absolutely fine. It is built into the system. We appreciate that, but, as someone who runs an ISP, the problem is that I have continually to assess threats to my business and threats to the operation of my network; and, at the moment, the Home Office turning up and saying, "You are going to have to start retaining this data", is classed as a threat. It is not that it might destroy our business, but it is going to take a lot of focus from my projects to provide service in rural areas or deploying the network in London. It is going to stop me concentrating on doing that part of the day job. There is absolutely no method in the Bill for recovering any of those lost opportunity costs, so I have to put together a pot of resources on the side, just in case. If the Bill specified exactly what I had to do, I could probably get to the point where I could put it into a background level, have a plan and know exactly what I am going to do and how I get from there to there; and, when the Home Office turned up with a retention notice, the actual process of

getting from the request to its being enabled would be a lot shorter as well, which, from an operational point of view, is beneficial.

Adrian Kennard: The key thing is that we do not have certainty in our business because we have this potential hanging over us. It is worth pointing out that the definitions in this Bill are very vague on who can be subject to these notices. It could cover schools, coffee shops providing wi-fi and it could cover businesses. They are all providing communications, albeit not as a business and not to the public, so for any business with any sort of IT department there is suddenly potential huge uncertainty over them with this Bill. It would be a lot clearer if the Home Office identified the operational requirements it has at the moment, which it has said are large ISPs, and the Bill pinned that down and said it has to be large communications providers.

Q120 Mr David Hanson: You will have heard the question I asked other colleagues earlier, which is, effectively, what your understanding of an Internet connection record is.

Adrian Kennard: The Home Office tried to explain it to us. Essentially, it was whatever you are ordered to collect, with huge scope for what that could be. We had discussions this morning when we were talking about event data, which seem to be about an event that does not have to have a place but has to have a time and at least one person and involve a communications service. If I have a conversation on the phone with a friend and say, "I am going down to the pub tomorrow", that is not an event, but if I say, "I am going down to the pub because they have really good wi-fi", that could count as event data because it relates to a communications service. It is so vague that, no, we do not know what it is.

James Blessing: The Bill itself does not make it clear. It is part of the concern we have raised repeatedly that, because it is not in the Bill, the code of practice has not been published and there is nothing else there, it is very much—

Mr David Hanson: Given that it is within a certain scope—we all roughly know, because the definitions on page 25 are what the Government think it should be, even if it is not nailed down yet—how easy do you think it is to do? If we said to you today that the Bill had gone through both Houses of Parliament and there was an implementation date of six months after it had gone through both Houses of Parliament, could you do it?

James Blessing: If you said that every telecommunications provider—it would cover an awful lot of people you did not realise it covered—was to be mandated that it must be able to record Internet connection records, it would be expensive. My network is not set up or designed in any shape or form to record this information, because I have as a business no need to do it; therefore, I would spend a lot of money on hardware. Six months is doable, but the other side of the coin is getting the data to law enforcement when it requests it in a format that makes sense for it. That is probably more work than installing new hardware across my network. I am going to have to send engineers to Cornwall and Aberdeen, but that could be done. It is about the actual amount of other things where we collate all that information and then present it in a format that works.

Mr David Hanson: Adrian, you are a smaller provider. How does that impact on you?

Adrian Kennard: You said the definition is in the Bill.

Mr David Hanson: It is on page 25 in paragraph 44, where they say what they think an Internet connection record is.

Adrian Kennard: That does not really define it, I am sorry.

Mr David Hanson: That is the general broad scope.

James Blessing: That is the problem. To somebody who does not run a network, it is too vague a definition of what is wanted. When do you connect to the Internet? Where does the Internet start, for example? Is connecting to your home network connecting to the Internet or is it only when you leave that that it becomes an Internet connection record? Is your phone auto-updating its software with no intervention an Internet connection record? By definition, yes, it is. There are an awful lot of things that would have to be recorded that you do not realise happen in the background.

Adrian Kennard: I think you are referring to 47(6).

Mr David Hanson: I am referring to the background notes, the Explanatory Notes in broad terms, on page 25, saying what they are after. It is not the actual legislation, just the background notes.

***Adrian Kennard*:** That is even worse.

James Blessing: That is the problem, because it is today's explanation, not tomorrow's explanation. Part of the reason that Internet connection records could be a problem is that, as the Bill is currently written, a Home Secretary in the future may decide to issue a notice saying that you must capture communications that happen over Skype, so you need to be able to identify which end-user talked to which end-user. It is not just that a Skype communication occurred, which we can do relatively straightforwardly, but which two end-users or multiple users were involved in that conversation. That goes into the dodgy territory of capturing third-party data because, as a service provider, I do not know which—

Q121 Mr David Hanson: Okay. We get the general idea. Given that the Government have established £170-odd million for this purpose, and it appears today that Virgin and BT are already planning to spend that amount, how much do you think it would cost you to meet the broad objectives that the Government are setting down?

Adrian Kennard: We are still stuck on the fact that it is a very broad objective, I am afraid. There are about three different levels of what we could be asked to do. If we already have a system that is logging some data for operational reasons, an email server that is logging emails that go through it, and we are keeping those for a few days to diagnose problems with the network, asking us to keep them for a year has some problems, but technically it is relatively straightforward and does not cost a fortune. There is a second level where we might have equipment that can be convinced to create some logs but does not at the moment, and that is a bit more work. The third level, looking into

the data as they pass through our network—where we are not the service provider for an email; where something is just passing through our network—is massively more expensive. It would double or triple our operational costs to have equipment that can look into the data as they pass through our network and extracts new information and logs it. The Bill has the scope to ask for that.

Mr David Hanson: I understand that you are a small provider. I do not know what that means in general terms, what your turnover is or how many contracts you have, but if the Government demanded that of you, how would you be able to deliver it, in terms of finance or—

James Blessing: Having vaguely sketched it—because I am a network engineer and it is sometimes an interesting exercise—in my bit of the business, which is the fixed line, not our parent company, our turnover is about £7 million. We have 40,000 or 50,000 end-users, so we are small in the grand scheme of things. You are looking in the order of £20 million to £30 million if I have to replace so much hardware on my network because it is not designed to do that; it does not have logging capability.

Mr David Hanson: Presumably if the Government do not facilitate your service doing it but do for BT, if I wished to be a child abuser, a criminal or a bank robber, I would use, with due respect, a smaller provider.

Adrian Kennard: That is a very specious argument, I am afraid. There are so many ways that anybody who is up to no good can bypass all this. They have no reason to go after a small provider. You cannot really trust that a small provider is not being monitored. It is possible that BT would be ordered to do some monitoring in the backhaul network that we, as a small provider, use. You cannot trust that monitoring is not going on somewhere in our service; it is just that we are not being asked to do it. Anyway, there is no need to. You just use any of the means to bypass this, such as Tor. At the moment even with things like iMessage you will not be able to see what is being communicated. Why would they bother trusting what a small provider says?

Q122 Mr David Hanson: The final point from me is in relation to access by the police. You will have heard other larger providers raise some points about access. How do you feel that would work in practice? Is what is suggested feasible? Do you have concerns about that or are you happy with the proposals?

Adrian Kennard: All this is about providing useful information to the police. The access is mostly a normal RIPA request, although there is the filtering facility and we still do not quite know what that will do. I am very concerned. We have experienced RIPA requests as an ISP, mostly about telephone numbers and some about Internet addresses. We have also experienced it as a victim of crime, when the police have been making requests of other providers to try to find our stolen equipment. Generally, we find that they struggle, even with modern communications. We had a case when one of our staff had to be an expert witness in a court case just to explain how phone numbers work, because they do not work in a simple way any more. My Bracknell phone number rings my mobile, my desk phone and my office phone. I seriously doubt, with that level of understanding, even with expert help, that the police will be able to make use of any sort of Internet connection records.

Even experts in the industry can have trouble keeping pace with the innovation and changing trends in usage. I do not think it is going to work well.

Mr David Hanson: Is the single point of contact officer—

Adrian Kennard: They are still not going to understand it enough.

James Blessing: Having dealt with a lot of single point of contact officers, they all have the right motives at heart and they are all trying to do their job. The problem is that they are policemen first, or other types of investigator. They do not necessarily understand the results. They also do not necessarily understand the implication of providing slightly wrong information. We have had a number of cases where the time zone was missing on a request; we get a request for a particular IP address asking who was using this IP address at this time and we reply saying, "At that time, it was that". Then they come back saying, "It could not possibly have been then". Then they work out that the time zone that they had recorded it in was in the US, and that was missing. It is little things like that. Until they do it for the first time, there are going to be a lot of mistakes. The filter may exacerbate that in the short term. Long term, it should make it better, but there is a massive requirement for training and support for the police and the single points of contact to be able to use it. There is an awful lot more work than has been put in and I do not see any funds in the Bill for that.

Adrian Kennard: I am also a bit concerned about how useless this information is going to be even when it is correct. One of the examples that has been touted by the National Crime Agency and the Home Office is about the possibility of a missing child and them wanting to get data about who the child was communicating with. They did not seem to realise that a mobile phone operator is going to be able to say, "Yes, that phone has been connected to Twitter 24 hours a day for six months since it was bought", but it does not tell you, "No, they looked on Twitter or they communicated with a friend on Facebook", because—

Mr David Hanson: It might do.

Adrian Kennard: No, it is going to tell you that Facebook has been connected 24 hours a day. That is how it works. Social media and messaging applications maintain a constant connection to the service provider. They do not wake up and say, "I have sent a message". You will find far more information about the missing child by asking their friends, because they tell everyone on social media. The ISP will not be able to tell that they chose to speak to someone at two o'clock.

James Blessing: On the comment I made before about when someone connects to the Internet, if you look at your phone now you will find it has updated your Facebook feed automatically in the background every few seconds. It is constantly doing it. You can tell that someone has a Facebook account, probably—

Adrian Kennard: But that is about it.

James Blessing: You do not know which Facebook account they are using, and you do not know whether they are actively using it or whether it is just that the software is installed and running. That is the best you are going to do in that situation.

Suella Fernandes: To follow up that point, you are aware that there have been very large-scale police operations that have been successful in large part because the law enforcement services had access to communications data or interception evidence. The Internet connection records can really help to provide a basis for further investigation, which can be critical.

James Blessing: Yes. I spent a couple of hours on Thursday morning helping a SPOC do some more research because they were not quite sure of what they had and they needed more evidence. I understand that completely. The problem with this is making sure we capture what is needed by law enforcement in a way that makes sense, so that it can interpret the information we provide securely and safely. It is not about not doing it at all. It is about asking what you actually need at the end of the day. The other problem you potentially are going to create is that, if you record all the records of every single connection that you are doing, stuff will be lost in the noise. You will start relying on data and say, "They were connected to there", when their phone might have been left in their bedroom turned on while they were somewhere the other side of town.

Q123 Suella Fernandes: I just wanted to make that point. A second question is about the security measures you use with the data that you have. Can you give us a bit of an idea of which mechanisms are effective for you?

James Blessing: As a company, we take credit cards, and there is a standard that we have to follow for that, which basically means the information is stored in an encrypted database with multiple levels of firewall protection. As far as we are concerned, if we were to do this, I would put the same level in place. I would do some checking. Part of the reason the filter is a concern is that you have to give third-party access to it, and it might need some engineering work to make sure that only trusted parties can access it, but that is a different issue.

Suella Fernandes: You say that firewalls and personal vetting systems are sufficient.

Matt Warman: Very briefly, it seems that a lot of what you have been saying is that there is a whole load of stuff that we may or may not need to record—some of that stuff about "When is your phone connected to Facebook?" All that I absolutely understand, but once we have nailed down the definitions that ceases to be your problem.

James Blessing: Yes. Nail down the definitions and everyone starts going, "Right, okay, now I can work out how to deal with it".

Lord Strasburger: I want to clarify Ms Fernandes's question. I presume she was referring historically to communications data derived from telecommunications rather than from the Internet. What you are saying—the view you are expressing, if I am hearing you correctly—is that the efficacy of the Internet communications data that are going to derive from Internet connection records is doubtful, as opposed to telephone communications data.

Adrian Kennard: Telephone communication is very clear-cut; it is the building block of the telephone network that telephone calls are made and everyone understands the concept and it is very clear. The Internet is not like that. Devices are constantly talking, constantly communicating with lots of different services all the time. Connections can stay running for days, months or years, and that is one connection. The usefulness of this is much more limited, with a lot more noise. It could be misused easily. It is very easy for someone to appear to be accessing services they have never heard of. I did a blog post today, and anyone who reads it will find they have accessed Pornhub because there is a tiny one-pixel image in the corner. They do not know that, but it will appear on the Internet connection record if they access my blog. That was deliberate, but there could be lots of things on websites, advertising networks and so on, that will create all sorts of misleading and confusing data even without someone trying to be misleading. As I understand it, in Denmark they had nearly a decade of trying to capture sessions on the Internet and abandoned it because they found it not to be very useful for law enforcement.

The Chairman: Ms Fernandes, did you want to come back on that other one?

Suella Fernandes: No. I meant how people are sending emails, what they are sending on the Internet.

The Chairman: I meant on the Information Commissioner.

Suella Fernandes: You are right; it was to follow up Lord Strasburger's presumption about what I meant in my question. I lost my train of thought. The question I wanted to ask initially was whether you think that firewalls and personal vetting services are sufficient for maintaining security.

James Blessing: Let us get this right. If operated according to design by the right people in the right way, yes. The difficulty is that operational procedures can drift away from perfect. It would not surprise me if there was a breach of the data stored in an Internet connection record at some point. It is not a question of if; it is a question of when. There will be a breach.

Adrian Kennard: Bear in mind that even the NSA, which has huge resources, had Snowden. It does not matter how well we do this, somehow someone will lose data; they will be breached and it will potentially be sensitive personal information.

James Blessing: As an example, the Home Secretary has possibly made herself a target for people who want to show that this is a bad thing to do; they may well try to go after her home service provider because they think that is a good thing to do.

Q124 Stuart C McDonald: You referred a couple of times in passing to filter requests. What is your understanding about how these are going to work, and what concerns would you have about their operation?

James Blessing: In theory, the filter is being described as a way of restricting the information recovered. That means that an automated system must be doing the requesting

of the data capture from the service provider and then presenting them to an individual. That means we have to allow third-party access to our systems, which is a potential risk. In theory, it would mean that the data was less open to fishing because you are only getting back specific results, but potentially there is a whole new construction of requests that people could start making, saying, "Who has visited Pornhub recently?" and Adrian's blog, and then putting that together, because it might be an interesting subset of people to go and do something else with. In some ways it is a good thing and in some ways it is a concern, because, again, the details are very limited.

Stuart C McDonald: It is the Home Office that would build the filter; is that right?

Adrian Kennard: I do not think it is specified.

James Blessing: Again, part of the problem is that it is not clear who operates which bit of the filter and how the filter would work. As far as I can tell from the information provided so far, it seems to be implying some sort of API access.

Adrian Kennard: Automated.

James Blessing: It is an automated access. Basically, a request comes in and it returns that information. How that happens in real life is not clear.

Q125 Lord Henley: Can I turn to Clause 189 and the ability of the Home Secretary to impose certain conditions on relevant operators and that these would come in the form of technical capability notices? I would like to hear what your views are on the ability of the Home Secretary to impose such a notice. How do you think your customers are going to react?

Adrian Kennard: My biggest concern is the removal of protection on communications. This comes down to the whole issue with iMessage, to some extent, in that it is end-to-end encryption at the moment. If providers are required, even secretly, to remove that protection, it removes all trust in those providers if they are offering a secure communications service but at any time they could be subject to an order that makes it not secure. That is a reason for companies to avoid being based in the UK and for customers to avoid UK companies. Encryption is a good thing; it is what keeps us safe from the very real threat of cybercriminals. If you got every communications provider in the UK, and even every foreign communications provider, to have this capability and to remove the protection they have provided, that still does not stop people, including criminals, communicating secretly. There are applications that do the encryption for you on your own machine when you send messages so that the provider cannot remove it. It is even possible to send messages that are completely secret—GCHQ could not get the information from those messages ever—just using pen, paper and dice. You could ban all computers and it would still be possible for people to communicate secretly. It is undermining trust and not solving any problems to tell operators they have to remove protections.

James Blessing: Most of the stuff is covered. The issue again is that it is not the Home Secretary who would be requesting that. It would be law enforcement because it needed to do something, which always comes down to this: most service providers are willing to

help law enforcement because, at the end of the day, we are part of a wider society. Forcing someone to go and break something tends to mean there has been a disagreement about doing something in the first place, and that is not a good place be to be.

Adrian Kennard: I have one other concern to do with the definition of communications provider. I have another hat today. I am a manufacturer, a UK business, making equipment that we sell round the world—a firewall router that would go in a small office. I am very concerned that there is the possibility that we could be asked to put in back doors or remove encryption as part of this. I think we would have to move the business out of the UK if the Bill goes through as it is at the moment.

Q126 Lord Henley: Now we turn to oversight and the proposed Investigatory Powers Commissioner. How do you see your relationship with him or her, and what changes would be appropriate when that office is created?

James Blessing: It is good that additional oversight is being created and put in place. That is always a useful thing to have. It is not clear from the Bill how independent a voice that person would have considering they are going to be appointed by the Home Office, pretty much, and they would be a judge. I am a bit sceptical that they would be as independent as their job title would lead you to believe.

Adrian Kennard: Yes. I have similar concerns.

Lord Henley: Finally, my Lord Chairman, I have one other question for clarity. I think it was Mr Blessing who implied that the costs imposed by the Bill, if enacted, could be such that his business would have to spend something of the order of four times your annual turnover.

James Blessing: Yes. Basically, the reason for that is that we have grown over time from a small organisation. We build the network small and then grow it, so there are no logical places within our network to do all the stuff that is required. We would have to go through replacing lots of pieces of hardware and upgrading them and their capabilities.

Lord Henley: Would that same figure, a factor of four, be as true both for small providers such as yourself and your membership as for some of the larger ones?

Adrian Kennard: It is difficult.

James Blessing: It is difficult. There are certain service providers where, because of their business model and the way they have built their network, it would be easy to do and it would not cost that much, but there are others in our situation where it would cost that. There are probably others where the multiplier is even higher. It will be variable because every network is different.

Lord Henley: The figure you were giving was one from your own experience with your own business.

James Blessing: Yes.

Lord Henley: It would not necessarily be true of all your members, but it might be higher or lower.

Adrian Kennard: Our business is different yet again. As James was saying, every ISP does things differently; it has different networks and will have different costs in doing things. In our business we make those FireBrick products and sell them to ISPs and use them in our network. It is entirely our own R&D in the UK and we have spent millions developing it. If we now have to change that to do different things, it could cost millions, or we scrap all our own work and buy in third-party kit, which would also cost millions. We would have to make major changes to do that.

Matt Warman: You talked about your fear that the Bill might ask companies to stop end-to-end encryption or that it might ask for back doors to be inserted. We have had the Home Office in front of the Committee saying that is not the case. The Home Secretary has said that on the Floor of the House. Are you saying that you do not believe them when they say that—

Adrian Kennard: No. But put it in the Bill if that is the case. It is as simple as that.

Matt Warman: The end of my question is whether you would simply like more clarity.

James Blessing: The issue is not the current Home Secretary or Home Office. That is the problem. It is that you have put it in the Bill; it is there. There are two things. It is in the Bill and therefore we are looking at it saying, "Technically, someone could do that". More importantly, someone outside the UK who trades with the UK will look at the Bill and say, "That technically says that they could do this".

Adrian Kennard: And "I am not going to deal with them".

James Blessing: I have two choices: this company in the UK and this other one outside, and I am a bit worried about that, so I will use the other company instead.

Adrian Kennard: We have already seen how putting too much scope in a Bill can be abused, with councils using RIPA to spot people going to a school outside their catchment area. I am sure the council thought, "We have got this power and we would be negligent not to use it". I suspect future Governments, Home Secretaries and Secretaries of State might well say, "We have got this power and we should be using it". Anything that is possible could happen. It is worrying.

The Chairman: On that very interesting note, thank you both very much. It was a very useful session, very informative. Thanks very much for coming along.

Witnesses: Jim Killock, Executive Director, Open Rights Group, **Shami Chakrabarti**, Director, Liberty, **Caroline Wilson Palow**, Legal Officer, Privacy International, and **Renate Samson**, Chief Executive, Big Brother Watch

Q127 The Chairman: A very good afternoon to you—or evening, now. I am sorry that we are a little late—there was a vote in the Commons earlier. You are very welcome. I will make two points before I ask the first couple of questions. My colleagues will come in after that. Each of you has given your response to the Bill very publicly over the last number of weeks. The Committee has all the statements that you have made. In addition, of course, I am sure that you will give us written evidence. This is a very big Bill. It is very lengthy and very technical. Has subsequent analysis of the draft Bill led any of you to alter any of your positions from those that were taken in your initial response to the Bill's publication?

Shami Chakrabarti: I would simply say that I am possibly more alarmed by the Bill than I was at first glance. The Committee will appreciate that it is a long Bill.

The Chairman: Very long.

Shami Chakrabarti: It is very complex. Like all legislation, it requires an understanding of what its clauses actually provide, as opposed to how its clauses have been pre-briefed or spun in the press. It also requires a level of understanding of the relevant technology. Those two things have to come together. My own organisation is a human rights organisation with, traditionally, considerable expertise in legislation, but recent weeks have given us the opportunity to work with partner organisations that have a considerable level of expertise in the technical sphere. That experience makes me more alarmed now about the personal and cybersecurity implications of the provisions, however laudable and well-meaning they may be in their motivation.

The Chairman: Do your colleagues share that view? Are you more alarmed now, as the weeks go by?

Renate Samson: Initially I was very clear that there was a lot to read. I have now read through it. The implication was that there was a lot of transparency. At first, it seemed that that was the case, but, as you read more and more, you find that there are a lot of vague terms in the Bill that require a lot of head-scratching to try to understand exactly what may be meant. Trying to engage the public in understanding what the Bill says and what its implications for them will be has been a challenge. There probably need to be many more readings of the Bill before you can get to the bottom of even a tip of what might have been meant.

Caroline Wilson Palow: I agree. We did and do welcome the opportunity to engage in this process. As we have started to get into the Bill, which is long and complex, we have started to notice a few things. For instance, Part 6 is about bulk powers, but when you look into some of the other particularly targeted provisions, you start to see that aspects of those look quite a lot like bulk powers in and of themselves. The service provider provisions that are sprinkled throughout the Bill put a lot of obligations on service providers, which I know you have often heard about, and which seem like they could undermine both security and trust. Those were not things that were necessarily apparent when we first took

a look at the Bill. Another particular provision that concerns us a bit is Clause 188, on national security notices, and how that will play out in conjunction with the other provisions of the Bill.

Jim Killock: We have been particularly alarmed by the reintroduction of the so-called filter, which complements the collection of very widely defined Internet connection records. The filter seems to us to be essentially a federated database and search system, very much like previous incarnations of the Communications Data Bill, the snoopers' charter or the intercept modernisation programme. It has been proposed a number of times and stopped a number of times, because of the power to look into people's lives that it would give. In a sense, that deserves an entire debate on its own, as does the recent admission of collection and use of bulk datasets.

What is a bulk dataset? Which of them have been accessed and grabbed by GCHQ so far? To whom might that apply? Just about every business in the country operates a database with personal information in it. It could be Tesco Clubcard information. It could be Experian's data about people's financial transactions. It could be banking details. It could certainly be any government database that you care to mention. From that perspective, it is hard to see where surveillance ends as a result of bulk datasets. Traditionally, we have thought of surveillance as being about communications data and as being targeted. In this Bill, we have various measures for blanket collection—bulk collection, as it is referred to—and we extend that to any private or public institution that happens to have data. From that perspective, it is pretty worrying. It is hard to see the start and end of it.

One good thing that we did not necessarily expect is that there is a thorough or, at least, a large document spelling out the apparent operational case for Internet connection records. The fact that that has been produced is a welcome step. A very important thing to do when asking for a new power is to produce documentation explaining why it might be needed. That said, it again requires examination on its own behalf, as do the GCHQ powers. They need an operational case. Parliament has not debated why GCHQ has those powers; it has merely been presented as something that is happening and that we should now legitimise. In the USA, those kinds of powers were examined—bulk data collection and use under Section 215 of the Patriot Act. An operational case was made and was reviewed by bodies that were trusted by the President and by the USA's democratic institutions—the Privacy and Civil Liberties Oversight Board and the NSA review board. Both came back and said that there was no operational case for the bulk collection and use of data; nothing the NSA had done showed that that data had prevented anything significant. That kind of review needs to happen here. The fact that it has happened in the USA and they have come up with the conclusion that these programmes need rolling back ought to be something that you consider carefully. Parliament really needs to examine those operational cases.

Q128 The Chairman: I think that I have got the message. I am assuming that you do not think that the Bill strikes the right balance between security and privacy. Without going into detail—my colleagues will ask questions on different parts of the legislation—other than dumping it altogether, do you think that it could be improved?

Shami Chakrabarti: It could certainly be improved. One thing we would all agree on, and would agree with the Government on, is that there needed to be a new Bill, in the light of

Mr Snowden's breathtaking revelations. Whether you consider him a hero or a traitor, there is no doubt that he revealed practices and capabilities where we, the people of great democracies on both sides of the Atlantic and all over the world—I would include parliamentarians in that definition of the people—had little or no idea of the sheer scale of mass surveillance that was being conducted against populations. There is a debate to be had, of course, about how much of that should or should not happen, on what basis and with what safeguards, but in the light of that there had to be new legislation, because whatever was happening was happening, at best, on very creative interpretations of outmoded laws. Some of us would suggest that it was happening outside the law and without sufficient parliamentary scrutiny, public discourse and legal authority.

We certainly agree that there must be a new Bill; there must be something like this Bill. My fundamental objection is that too much of it is about sanctioning mass surveillance of entire populations and departing from traditional democratic norms of targeted, suspicion-based surveillance, for limited purposes. There are insufficient safeguards against abuse. For example, there is the argument that I know you have had extensively about the role of the judiciary. Our position is clear. This is not a system of judicial warrantry. This is Secretary of State warrantry, save in one of the most chilling provisions of the Bill, which is about hacking and the new concept in public understanding of what the authorities propose to do. We think that is one of the gravest powers, because potentially it leaves long-term damage to systems, individuals, devices and security, after a perhaps justifiable investigation. That has the lowest safeguard of all, because in certain circumstances it involves not even the Secretary of State but, for example, a chief constable. There is too much surveillance, there are too many people, it is not to a tight enough threshold or a high enough standard and there is insufficient authorisation by the independent judiciary.

Caroline Wilson Palow: Following on from that and your introduction to the question, security and privacy are not necessarily mutually exclusive. The hacking provision, in particular, shows that there is a lot of potential to undermine security by allowing that power, including the fact that the use of malware—the type of software that allows access to computers through hacking—is not necessarily well controlled. It is like breaking a lock on a door and leaving the lock broken, so that other people can potentially get in and access the same device or equipment that was targeted in the first place. That is an example, within equipment interference, of some of the security problems. There are also greater, overarching concerns about undermining things like encryption standards and whether or not that would be permissible, both under the hacking provision and under some of the provisions, like Clause 189, which say specifically that the removal of electronic protection could be required of service providers that are subject to compliance with warrants and authorisations under the Bill. Finally, data retention in and of itself has certain security concerns. Of course, as we have recently seen with TalkTalk here or even the Office of Personnel Management in the US, there are breaches. When you are mandating companies or even Governments to keep more information, it makes the breach even worse when it happens.

Renate Samson: I support the points that have been made about concerns with regard to safeguards. Caroline made the point that privacy and security are two sides of the same coin. We also have to look at the idea of protection. Part of this Bill is about protecting the public, yet, as has been pointed out, there are other elements that will potentially make the

public vulnerable, whether that is through equipment interference or through weakening of encryption, for example. We have to step back and have a think about what protections the public require with regard to the proposals in the Bill. The idea of full independent judicial authorisation is something that I know you have been discussing at length. I would support the view that it needs to be explored in a lot of detail. We are on the cusp of being complete digital citizens. We do not have a choice any longer about our engagement online. Proposals that suggest that online engagement can be surveilled at any time, potentially, and retained for a number of months are a worry to us all. It is not the case that the Bill should be scrapped, but there are certainly areas that need to be strengthened greatly.

Suella Fernandes: On the flipside of those comments, do you equally accept that the scale and nature of the threat that we currently face is unprecedented and severe?

Shami Chakrabarti: I do not doubt that the world faces enormous threats from crime, terrorism and so on. I do not think that any of us doubts that. The question is how best to counter those threats. I will repeat the previous remarks, which are really important. It is not about a trade-off between privacy and security. A lot of what we are concerned about is actually security. What is national security if not the personal and, increasingly, the personal cybersecurity in relation to where I am—whether somebody is in my house, engaging online, and whether I am away and, therefore, open to an attack or a burglary? My financial records and so on are part of my personal security and cybersecurity. National security is to some extent the combined personal and cybersecurity of millions of people. We think that up to 50 billion emails are intercepted every day by UK authorities. There are only 7 billion people in the world, and only 3 billion of them currently have access to this kind of technology. To me, that in itself is a threat to personal security—not because the authorities are malign, but because when you collect data and create vulnerabilities, that data can be attacked by non-governmental sources and the vulnerabilities that have been created can be attacked similarly.

Suella Fernandes: On the vulnerabilities you talk about, you point out the scale of, for example, communications data and equipment interference and interception, but those powers have been absolutely essential and critical to successful convictions for large-scale child sexual exploitation, human trafficking and serious and organised fraud and crime. Those are powers that are currently exercisable by our law enforcement services. The Bill represents a drawing together and consolidation of existing powers.

Jim Killock: We are talking about several different things here. There are policing powers, there are data retention powers and there is extension of those for the police in the ICRs and the filter, so you have that body. Then you have the other area around GCHQ—what it does and how it gathers information. You have to look at both of those quite separately.

You are really asking about the operational case. As I said, my problem with the operational case is that it has not been presented to anybody for GCHQ. When the equivalent was done in the USA, the President of the USA and its democratic institutions decided that there was not really a case for a lot of it and decided to roll it back, because it was essentially purposeless. Here we have an operational case for the police with regard to ICRs, but we do not have the mechanisms, because we do not have a civil liberties board

in the UK. It has not been constituted, despite potentially being put into law. That has not been examined.

On data retention in general, we have had a ratcheting back of data retention in a lot of Europe. These apparently essential tools have not been operational for a long time in Germany, the Czech Republic, Slovakia and a number of other places. There are about six or seven countries where these sorts of programmes have essentially been cancelled. There has not been a concomitant outcry from the police that they are no longer able to solve crimes and that there is spiralling dysfunction in the police. That has not occurred. Something to bear in mind is that there are often several routes to solving crimes. Data, through data retention or collection, is only one. That data probably resides on laptops and mobile phones. It will reside at service providers. That is talking only about the data side of it; there will be other kinds of factors in the equation. It would be interesting to hear from Caroline about data preservation and the standards elsewhere.

Caroline Wilson Palow: The US, for instance, does not have a data retention provision, yet it is still able to solve crimes. In fact, it uses mechanisms like data preservation orders, which are much more targeted, are not across the board and can be quite effective. You also have instances, which have been mentioned, of places like Germany, the Czech Republic and other countries in Europe where data retention is either much more circumscribed or non-existent. Again, we have not seen a collapse due to the fact that it is not there.

To pick up another point you asked about—the existing powers, particularly in the context of equipment interference—it is true that it was revealed earlier this year that the intelligence services were engaging in hacking and, when this Bill was introduced, that law enforcement, too, was engaged in hacking. Until that point, that had not been revealed publicly. The reliance on the Intelligence Services Act and the Police Act, which are incredibly broad powers, to say that that was already in statute is inappropriate, because they are so broad. There was no indication that it was actually happening. Since those Acts are from 1994 and 1997, if there was an indication in the Acts that hacking was possible, why was there concern not to reveal it sooner? Why was the position of the Government until earlier this year neither to confirm nor to deny that those powers were being used? While they may have been in use, they have not actually been in law up to this point. That is why we talk about them as new powers in this Bill.

Shami Chakrabarti: I have one further small point on comparative practice around the world and the importance of law enforcement. There is still no provision for intercept evidence to be admissible in criminal proceedings. There has been and is to be all this interception, for laudable criminal justice purposes—public protection and law enforcement—but there is still not the provision, for which some of us have asked for many years, for interception, when it is proportionately and lawfully gained, to be used in criminal prosecutions, as is the case all over the democratic world and among our allies.

The Chairman: Thank you. I move to Dr Murrison.

Q129 Dr Andrew Murrison: I am getting the sense that you are not convinced that the "double-lock" provision, about which much has been spoken in recent weeks and on which

much store has been put by those who have been involved in bringing the Bill to the position it is currently at, is really much cop. However, I believe that it is likely to remain a feature. Given that it is likely, what do you think could be done to improve the double lock? Would you see virtue, for example, in distinguishing national security from serious crime, having the double lock apply to national security and having judicial authorisation only for serious crime? Would you see virtue in, for example, a different means of appointing the information commissioners who will be involved in this process?

Shami Chakrabarti: Some of my colleagues are the great technologists and experts. I am just a humble lawyer in recovery—or in remission—so I find it easier to make the analogy with the real world when I am dealing with the virtual one. We are digital citizens, but we are still people and citizens. If I want to search your house or your office for laudable reasons, I go to a magistrate for a warrant. I can understand the argument coming from the Government that when we are doing this national security stuff and, perhaps, spying on foreign Governments, we cannot just go to any old magistrate. There has to be a double lock, surely, on something as serious as interfering with the German Chancellor's communications. That is such a political decision that there ought to be some Executive involvement. The double lock is simple: have a provision across the board for judicial warrantry, but as an internal administrative matter, make sure that those warrants are not sought by the authorities unless they have been to the Home Secretary first. In the non-crime cases—the international relations/national security cases—as a matter of good public administration, go to a Secretary of State first, but always have the sign-off to protect people's rights and freedoms, whether in the UK or around the world. Have that sign-off by a judge, as you would for your home, your flat or your office. Again, that is the practice across the democratic world.

Renate Samson: I second that. A large part of what we find ourselves doing when it comes to the digital world is incomprehensible to most of us, because it is invisible, yet we all understand what happens when somebody knocks at our door and asks to have a look around because they suspect us of something, and that element of being suspected of something is important. The real world understands a judge signing off on something. The general public have confidence that there is independence to it. While we may currently have a benign Government, we do not know what the future holds. This piece of legislation should hold up for many years. We do not know what the future will bring, so independence is hugely important. That will also mean how the judges are appointed. To feel genuinely that surveillance conducted upon us is being assessed independently and with no interference from anywhere else will reassure the general public that, should the rest of the provisions in the Bill become law, they will be secure and thoroughly thought through, not just signed off with a flick of a Minister's pen.

The Chairman: It is said that a Secretary of State is ultimately accountable to Parliament for his or her actions, whereas a judge is not. What is your view on that?

Renate Samson: You took evidence at the beginning of this week from Mr Paterson and Lord Blunkett. I think that they answered that question for you, in that neither of them has ever stood up in Parliament and talked about a warrant they have been involved in signing off.

Jim Killock: It is also worth reminding ourselves how we got here, in a sense. The Regulation of Investigatory Powers Act had powers for the collection of material from persons overseas. The meaning of that warrantry system was extended through practice to mean every communication passing between the UK and the USA. That is how the Tempora system of bulk collection was created—through those warrants, which were politically authorised. There was a political decision, alone, to extend the meaning of those RIPA warrants, which meant that essentially Parliament was cut out of the decision, right or wrong, to engage in the programmes of bulk collection of data that we are now authorising in this Bill. It seems to me that if one is to restrain the Executive from creative interpretations of the statutes, as Shami said, you need that judicial authorisation. They should be saying, "Minister, I do not think that this is necessarily how the system was designed to work. Perhaps you might like to consult Parliament". That is a far more likely outcome than the Home Secretary saying to GCHQ, "No, I am going to deny you those powers for one or two years while I work out a political opportunity to legislate".

Caroline Wilson Palow: In conjunction with that point, it means that the judicial commissioners need the full ability to assess the warrants when they come to them. It should not be just a judicial review standard. They need to assess fully the substance of the warrant and, among other things, whether there are other less obtrusive means by which this information could be obtained. That is an easy edit to the Bill. Every time the judicial review provisions appear—it is at subsection (2) of most of those clauses—you just delete it. You take it out.

Suella Fernandes: Are you saying that the double lock and the judicial involvement strike the right balance in having judicial review as an element of the decision-making process, or are you saying that it should not be there?

Shami Chakrabarti: Judicial review does not help at all in this context. When you are deciding whether it is proportionate to issue a warrant for intrusive surveillance of an individual, let alone of a whole group of people, that is a judgment made on the evidence. A judicial review test only second-guesses the Secretary of State, in very limited circumstances. Did they make a bonkers decision that no reasonable Secretary of State could take? That is not judicial warrantry. In the statute there should be a one-stage test: the judge signs the warrant. However, because people are concerned about cases of interception on foreign powers, for example, which is classically a matter for the Executive rather than for independent judges, police officers or whatever, interception and so on of foreign statesmen and powers should go to the Home Secretary first, as a matter of good public administration. You would not even need that in the statute, or you could put it in the statute for that category of case.

Renate Samson: Your question is interesting. I have listened to a number of the sessions of evidence that you have taken. You have all posed the question a number of times, "What exactly is meant by judicial review?". Witnesses have given you a variety of versions of what judicial review means. There is lack of clarity.

Suella Fernandes: That is exactly what I was going to raise in my question. You will agree that, with judicial review, the judge would have access to the same information as the Secretary of State or the Minister.

Shami Chakrabarti: I do not think that is suggested in the Bill. There is nothing to suggest that.

Suella Fernandes: That is what judicial review involves, does it not?

Shami Chakrabarti: No, it does not. This is a term of art. A judicial review test, as a matter of our law, is a very limited opportunity for a judge to second-guess a decision that has been made by a public authority, whether it is a Secretary of State, local government or whatever. It is not a double lock.

Jim Killock: Basically, it is, "How did you follow procedure?", is it not?
Shami Chakrabarti: Yes. Did you make a decision that was within the realms of a reasonable decision? Could any reasonable Secretary of State possibly have made that decision? It is not appropriate for warrantry.

Suella Fernandes: What about the proportionality test, which involves balancing the right infringed and the objective met? That goes further than what you are suggesting, does it not?

Shami Chakrabarti: But that has not been allowed to the judge, under the provisions of the Bill. They are not second-guessing the Home Secretary's decision on the merits of proportionality, under the Bill.

Caroline Wilson Palow: That is exactly our concern. When you talk about judicial review, all you are doing is looking to see whether proportionality has been assessed by the Secretary of State. The judge will not have the power to say, "You have made that assessment incorrectly". In the US, to give an example of a comparison between two different types of warrantry there, a normal warrant would go directly to the judge. There is a political consideration that is made ahead of time. For instance, the US attorneys, who are the federal attorneys who often start the process, are politically appointed and will make a decision about whether or not to seek a warrant in the first place. Once that is done, it goes directly to the judge.

Suella Fernandes: Before we finish this line of questioning—I know that other people want to get in—I need to put on the record that the statute states explicitly that it must be "proportionate" and "necessary". That is the relevant test.

Shami Chakrabarti: You have to look at Clause 19(2).

Caroline Wilson Palow: The concern is the way in which the two play together. That is why I said that we think you should just delete subsection (2). We totally agree that necessity and proportionality need to be assessed, but, once subsection (2) is in there, it reduces the ability of the judicial commissioners to make that assessment. To continue the parallel that I was trying to draw, in the US there has been a lot of talk about the FIS Court, which acts on foreign intelligence. This is PRISM—the types of authorisations for collecting intelligence on people around the world. Its powers are the equivalent of what judicial review would be here. Essentially, when a request comes to it, it has to check the box to say that everything has been considered as necessary, but it does not necessarily get

to question the conclusions that were reached by the person who was seeking the warrant in the first place.

Shami Chakrabarti: A double lock would mean, "I can substitute my decision on the merits for yours". Traditional judicial review means, "I look at the way you made your decision, but I do not substitute my own for yours". You have to be procedurally irregular or to have made a completely insane decision that no Secretary of State could make. That is achieved by Clause 19(2), otherwise there would be no purpose to it.

Matt Warman: We have had an awful lot of witnesses tell us that their expectation and understanding of what the Bill says regarding judicial review would, as Suella Fernandes has said, in fact mean a test that looked at the evidence. It would have to be proportionate and go through all those things. You are saying simply that that is not your understanding of judicial review. It therefore seems to me that we are talking simply about definitions; we are not actually talking about a principle, because what we have been told is what you are saying you are asking for.

Shami Chakrabarti: It just does not stand up in law. These are well-tested terms. If you want to create a full merits appeal in statute, there are many precedents for doing that. You do not put in a clause like 19(2); you can do it much more simply. I believe that you will hear from the Secretary of State in the not-too-distant future. You can just ask her: "Is it your view that you will make an initial decision and there will be a full merits review? The judge can just second-guess your decision and make a different one. Is that your intention?". If she says that that is her intention, that will help for Pepper v Hart purposes, but there are far clearer ways to deal with it, like just deleting Clause 19(2).

The Chairman: Thank you. Can I move to Mr McDonald?

Q130 Stuart C McDonald: I have another million-dollar question. What is your understanding of the meaning of the term "Internet connection record"? Why would their gathering and analysis be more intrusive than for other forms of communications data?

Shami Chakrabarti: This has been quite a journey for me. I have had lots of younger and more technologically savvy colleagues explain the sheer scale of what we might be looking at as regards Internet connection records. If you take your favourite device—your smartphone, your tablet or just the sites you go to from your laptop or desktop—we are looking at things like the websites you visit. We are looking at the communications software that you might use to speak to your mother—Skype, WhatsApp and so on. We are looking at all the icons on your menu, such as your Twitter and your diary. Recently a health one popped up on my phone uninvited, telling me how many steps I took yesterday. Taxis, maps; the list goes on. Photos, my Internet shopping, banking apps—I understand that all those things are potentially within the broad concept of Internet connection records. As we look just a little way into the future, in the discussion that people describe of the Internet of things, more and more of our real lives will be managed online. Now we will be talking more and more about the little icons on our devices that connect to our fridges, our cars, our burglar alarms, our gaming devices and so on, so the separation between my real-world security and privacy and my cybersecurity and privacy is almost completely collapsed. This is very intrusive on millions and millions of, for the most part, completely innocent people.

Renate Samson: It comes back to the point that I made that we are all now digital citizens. It is that—it is life. It may feel at the moment that it is just a mobile phone and a laptop, but, as Shami explained, with the Internet of things it will be everything. That will create a huge amount of data that will be constantly ticking over. We have been informed that the Internet connection records are just the URL, before the first slash, of a website and no content, but from the technical evidence I have been listening to and you have been receiving, and from all the different things that I have read, which Jim will probably be able to explain better, I am not entirely sure that it is quite as clear-cut as has been implied. I would certainly like to hear from the Home Office—from government—with regard to this Bill a very clear definition that it knows exactly how this can be done, because I am not sure that I do.

Jim Killock: It seems to me that essentially the Internet connection record starts from the point of view that the Home Office wants the power to have retained the fact of somebody using the Internet, with some other service, and to record that. It has decided that the best way to do that, given how much the Internet is used, the purposes it might be put to in the future and the services that might appear, is just to say, "Let's have a very broad definition of anything that connects to anything, whether it is a person or a machine. That will allow us to compel Internet service providers to collect information about anything we deem important in the future".

I do not think that is really a good way to legislate. It is incredibly broad, it is open to abuse and the cost implications are impossible to put a number on. If you have power to collect and retain any information, no matter how difficult that is and how much of it there is, essentially you have just written a blank cheque to scale up surveillance indefinitely. Of course, once you have an initial investment and the thing has started to roll out, that poses the problem of how you restrain it in the future when it turns out to be not quite as useful as you hoped. Do you pour in another few tens of millions of pounds to extend the amount of information that you are collecting under this very broad power? Given that the companies will probably tell the Government that it will be more effective if they spend that extra bit of money, this seems to be a financially haphazard way of working, as well as haphazard in terms of human rights and the proportionality of the surveillance we are authorising.

Caroline Wilson Palow: This is quite a confusing definition, because essentially you have two different definitions in the Bill. You have Part 3, where Internet connection records are explicitly mentioned, but in Part 4, under data retention, you have a clause that, under the commentary, is supposed also to encompass Internet connection records. The definitions do not completely align, and for that reason we are somewhat confused about what Internet connection records really are.

Let us take an example from the commentary that Renate has already mentioned—the idea of taking the domain name of a website, which is the information before the first slash. Potentially, that could be quite intrusive and could reveal a whole lot of information. It is not as innocuous as just bbc.co.uk, which is the example that they gave. For instance, that domain name could be saveyourmarriagelikeme.net or domesticviolenceservices.com. Maybe one of the most interesting ones is crimestoppers-uk.org. This is where you can

make anonymous tips to help to solve crimes. Of course, if you had the Internet connection record that said that someone had gone to crimestoppers-uk.org and you also knew the time when the tip had come in—if you were the police, for instance—you could very easily figure out who had put in that tip. That is a real problem, because if you are destroying that anonymity you can undermine the ability to solve crime.

Q131 Mr David Hanson: This is the central question many of us will have to wrestle with. Surely the police, the security services or whoever accesses that, under authority, with judicial review, is doing so only because there is some potential link to a potential investigation. The vast majority of people will never have that link checked or looked at. I am wrestling with that myself. I want to get your assessment of whether the proportionality is there. If we do not collect the information, none of those leads can be followed up.

Shami Chakrabarti: You are collecting huge amounts of sensitive information that is not currently collected and, therefore, you are creating the vulnerability I am so concerned about. I am not even talking at the moment about potential abuses by the authorities. I am talking about the vulnerability to hacking by other people that you create when you create a massive sensitive database and put the entire population's online life under surveillance in this way.

Renate Samson: My understanding is that this would help to support requests that are already made for communications data. At the end of November, IOCCO published as a starting point to a further publication a breakdown of 100,000 communications data requests by 29 police authorities, including the National Crime Agency; 46% of those requests related to burglary, robbery, theft and drug offences. If this is to support that, people may see it very much as an intrusion. On that sort of issue of crime, why do you need to know what website somebody has looked at with regard to burglary? We have to think about the intrusion into people's lives, based on us as digital citizens, before we start to discuss the retention and use of Internet connection records. Their retention is an issue I know you have looked at, but off the back of the TalkTalk hack, for example, we need a lot more clarity on how companies will be asked to store that data to ensure that they are safe.

Jim Killock: You also have to consider the wider effects on society. If I said to you, "When you go home, can you note when you got home and which newspaper you read, although do not worry which article it was? If you ring your family this evening, make a note of that and then tomorrow, hand it into the police", you would think that an excessive ask.

Shami Chakrabarti: And every hotelier, every restaurant owner, every pub, every cinema and every theatre that you enter will be required to keep a record of when and where you entered. That is the equivalent of what is being proposed.

Jim Killock: The question then is, is that a proportionate thing? What are we trying to solve? Is it quite as desperate a situation as is being claimed? As I said, these powers do not exist in other democratic countries. Russia has just been given a bit of a rap for similar sorts of activity. A number of European countries have rolled back on traditional data retention, never mind this kind of extension.

The Chairman: Lord Strasburger?

Lord Strasburger: My point has just been covered.

Q132 Stuart C McDonald: Are there other ways to go about IP resolution that are less troubling? The Home Office and law enforcement agencies will say that retention of these connection records is essential for that to be successful.

Jim Killock: One thing that you have to ask is whether the technology will out-evolve this. Will IPv6 catch up with some of the problems that it is currently seeing? You also have to ask how the Internet might work in the future and whether any of this will work. Some of the evidence that has been put about is quite interesting. People have said, "How do we know whether somebody has used Twitter or Facebook? We need to know in emergencies whether somebody has been accessing that website". Phones just do that now every couple of minutes. If they are constantly connecting to all these services, you will just have a huge glut of information that is not a fat lot of use to anybody.

Q133 Matt Warman: One of my frustrations with this conversation is that it is always said that the Government are being asked to hold this stuff. Actually, we are asking ISPs to hold it. That is a very important distinction that we need to continue to make. Law enforcement agencies tell us that they want access to the information and are happy for it to be held externally. You seem to be saying that you are not happy with that. I wonder what alternative you would propose.

Jim Killock: It may not be a government-held database, but it is a series of data centres that are all accessible by a single mechanism that can then be queried in parallel from an officer's desk.

Matt Warman: With appropriate oversight.

Jim Killock: There are some interesting things there. It seems that the way it will work is that you can get an officer to ask the computer whether it has any useful information in a case. It will tell you the things that it might have, and then you can go off and get some warrantry for it. It is almost saying, "We will go not on fishing expeditions, but if you did, here are the results you would get. Why don't you have a think about whether or not that is useful?".

Renate Samson: You say that there will be appropriate oversight. Currently the Bill will retain the process that we have now. From Big Brother Watch's point of view, that is not appropriate oversight. We would like to see a further layer of independent judicial approval and authorisation of an internally signed-off warrant.

Matt Warman: The point I was making is that it is not a free bucket any policeman can look at.

Renate Samson: We also have to acknowledge the recent case with regard to Police Scotland and on which IOCCO reported, where warrants were being signed off and misused.

Matt Warman: Misused being the operative point.

Renate Samson: Yes.

Shami Chakrabarti: Sometimes that will happen. To go back to the real-world analogy, when I said that this is the online equivalent of requiring all those businesses—hoteliers, restaurants, cinemas and so on—to keep a detailed record that they do not currently keep of everybody's comings and goings, that does not mean that I am against ever putting a particular hotel, restaurant, gym or whatever under surveillance. I just think that you take a targeted approach. When you get suspicion that conspiracies are being conducted in a particular room above a particular pub, at that point you put that site under surveillance. Then you put the people who have been to that site under surveillance. That is the kind of approach we should continue with in our democracy, in the virtual world as well as the real one. If you have concerns about particular activity and sites, you can go to ISPs and CSPs and ask for the data they currently hold anyway. You can seize people's devices, because those people or organisations have now come under suspicion. You can target suspicion not just around individual people but around organisations and, indeed, websites.

Renate Samson: I want to clarify your point about misuse. IOCCO is very clear that judicial approval was not obtained to acquire the communications data. My point, and the point of Big Brother Watch, is that independent oversight and authorisation of an internally signed-off warrant for communications data would, I hope, potentially ensure that misuse did not occur. That is just for clarity.

Jim Killock: The important thing is why we have the idea that necessary and proportionate surveillance is essentially targeted, rather than blanket. Why do we have that rule? Why has that been pushed forward? It is easy to imagine that in the UK we will never have any problems with our democratic institutions, the police will never overstep the mark and we can solve all this through authorisation regimes. However, if you look over the sea in France, you have the potential of a Front National Government, with parallel powers. You have powers similar to these in China and Russia. Is it the role of the UK to say that blanket surveillance, easy profiling and access to everything that everyone does in their lives is the right international standard to set and is absolutely, 100%, guaranteed never to turn into a problem in this country, or should we restrain surveillance to somewhere we can trust, for ourselves, for other people and for the long term?

The Chairman: Can I move to Lord Butler?

Q134 Lord Butler of Brockwell: I want to ask you about equipment interference. You have made reference to that. As I understand it, you are not claiming that equipment interference in the past has been non-statutory. You are claiming that, although there are statutory powers, they are very general, they have been widely interpreted and the public have not been aware of what is going on. Do I have your argument right?

Shami Chakrabarti: You do have my argument right. I do not believe that equipment interference was necessarily in the mind of the legislators when the provisions that are

now being relied on were passed. Those provisions were more about traditional breaking and entering, bugging and so on. I certainly do not think that the public understood in that way the activity that was being justified ex post facto. That creates a problem for Article 8 of the convention, which requires a certain level of public understanding for something to be law for the purposes of the ECHR. Those powers were there and they were used for more traditional interferences, but hacking is a very, very serious business. It is more than just surveillance, because you are potentially changing data and causing long-term damage to data security. I am not saying that it should never be allowed, because that would be like saying that you should never break and enter in order to find the hostage, the terrorists and so on; I just think that there should be much tighter safeguards for hacking in the Bill. Again, in principle, it should be a targeted approach, not a blanket one.

Jim Killock: It is worth remembering that the hacking power has already caused some very significant problems. You probably remember that Belgacom, the telecoms provider in Belgium, was hacked by GCHQ, allegedly. In the first month of the clean-up, that cost it around £15 million. A series of telecoms providers, including Deutsche Telekom, were also hacked by GCHQ. Those are law-abiding companies. They are not terrorists. They have information and are a conduit to further information, perhaps, but they are also people who can be compelled to co-operate with their own national authorities. However, GCHQ, under this warrantry and hacking regime, has instead taken the view that foreign, legitimate companies with international stature, within the bounds of Europe where we have common laws and systems, are a legitimate target for hacking, and that the clean-up operations are, frankly, not our concern.

Lord Butler of Brockwell: Could we stay within the UK for the moment?

Jim Killock: But this is a UK operation.

Lord Butler of Brockwell: I know that it is a UK operation. I am just talking about the targets at the moment. The point that you have made is about overseas targets. That is a separate consideration. Within the UK, you must agree that it is an advance that this proposed Bill gives specific authority for and introduces transparency into that power.

Shami Chakrabarti: I agree with that. I would just like it to be more tightly regulated, given the consequences.

Lord Butler of Brockwell: Sure. You are not arguing, are you, that such a power, properly warranted—we have had discussions about what proper warranting is—may not be a legitimate weapon?

Shami Chakrabarti: In extremis. The intrusion is graver, because it is not just surveillance but actual damage—not least, potentially, damage to fair trials, if now every criminal defence lawyer can argue, "This isn't a genuine email. This isn't genuine data any more, because of hacking capacities". Given how serious the consequences of hacking are, the thresholds possibly need to be even higher than for other powers in the Bill.

The Chairman: I will now move to Lady Browning and Lord Henley. I am conscious that there is a vote in the Commons at 7 pm, but I would very much like the Commons members to be here for the questioning.

Q135 Baroness Browning: You have all expressed concern about Clause 189. I wonder whether you could share with us what you believe the effects will be on both service providers and customers. Ms Wilson Palow, your submission stated very clearly your concern about this.

Caroline Wilson Palow: It is a very broad power, to begin with. Essentially, it says that obligations can be placed on service providers to facilitate interception, hacking or any other power in the Bill, and they would need to take those steps ahead of time, before an authorisation or warrant was placed. Within that broad power, there are some examples of what might be done. A particular concern of ours is the removal of electronic protection. We interpret that as the potential to undermine encryption. Encryption is crucial to so much of what we do all the time, including all our financial transactions. It gives us the security to operate online. The removal of encryption has the potential to undermine all of that. We think that the balance there has not been struck appropriately.

Shami Chakrabarti: Taking my real-world analogy again, because of my poor understanding of these things, I do not think that it would be proportionate to give government the authority to demand that every locksmith in the country makes a spare key every time he is setting a lock for a home, a property or whatever. It is proportionate in certain circumstances, under warrantry, for the authorities—the police—to break into a targeted property because we believe that there are explosives, contraband or evidence there. To ban privacy, to ban private conversations and to require people who live on trust—companies that are all about creating a space of trust, so that we can have trust in our banking system et cetera—to leave those gaps in the nation's cybersecurity is quite problematic.

Renate Samson: It is the point that we were making earlier. The Bill is about protecting society. Encryption enables the protection of society. It enables people to use Crimestoppers. It enables whistleblowers to lay clear things that are going on that benefit society. It enables the vulnerable to communicate safely. Battered wives, for want of a worse expression, can ensure that they communicate as necessary. People on witness protection programmes can have an element of safety. It is much broader. It involves all of business. When all the communications in our home and everything else we have talked about on the Internet of things are connected online, we all want to know that our energy can be supplied safely. Encryption, as our submission to you explains, is not just a concern of privacy campaigners. It is a concern of Governments and business and one that will impact on us all, as all our lives are lived online.

The Chairman: Thank you very much. I move now to Lord Henley, on the Wilson doctrine and other matters.

Q136 Lord Henley: There is protection in the draft Bill for legally protected communications of journalists and journalists' sources, and there are protections for Members

of Parliament of both Houses, enshrining the Wilson doctrine. Do you think that the Bill goes far enough?

Shami Chakrabarti: Not at all. There is room for some serious improvement. Let me be positive: there is room for real improvement. As far as I can tell, the Wilson doctrine has been completely reneged on. Recent statements by the Prime Minister suggest that, effectively, there is no Wilson doctrine in practice any more.

Lord Henley: What particular comments of the Prime Minister are you referring to?

Shami Chakrabarti: My understanding of recent statements from the Prime Minister is that there is now no absolute practice of not intercepting parliamentarians' communications. That was an absolute promise that came from Prime Minister Wilson and, indeed, was repeated by subsequent Prime Ministers.

Lord Butler of Brockwell: No. I am sorry, but you are wrong about that.

Shami Chakrabarti: I have read the Wilson statement. As regards what could be improved, I accept that there could be certain very rare circumstances where it would be justifiable, in a democracy, to interfere with even the communications of parliamentarians, lawyers and journalists, but we want something closer to the provisions that you currently have in place for production orders. You want something approaching reasonable grounds for believing that a very serious criminal offence is happening or has happened, and that there are no alternative ways of getting to the evidence; otherwise there are real dangers. Think of the political dangers. Perhaps it was just a rhetorical flourish, but we have had leaders of parties suggest that opposition parties are a threat to national security. I do not think that it is healthy for democracy for opposition political parties to believe that it is possible that they can be intercepted just on the say-so of a political opponent, even if that political opponent is the Prime Minister.

When it comes to legal professional privilege, we now know, because of the Belhaj case, that the security agencies were looking at legally privileged material that was relevant to a case being brought against them in relation to torture. There need to be much graver safeguards—we are back to judicial warrantry—and a very strong presumption against looking at parliamentarians' communications, legally privileged communications and journalists' sources.

The Chairman: Thank you very much. I will give you just one or two more minutes, because I want to wrap up with a couple of suggestions about how you can give us more evidence.

Jim Killock: I want to say something very specific about this. It is very hard to tell where the boundary between journalist and non-journalist lies. In this day and age, it is not somebody who is working on a paper; it could be somebody writing a blog and self-publishing. Many NGOs have a similar role to journalists in exposing, commenting and publishing. Particularly with communications data, where the system sometimes has to go to a magistrate or whatever and sometimes has to be self-authorised within the police, it breaks down when you have this blurring, which is a very strong reason why all authorisation should be done by an independent authority. That, in particular, has been

spelt out in the data retention judgment by the CJEU; when communications data are accessed—in that case, it was talking about retained data—there should be independent authorisation. This is one of the reasons why.

The Chairman: Thank you very much. It has been a fascinating session. It really has—very revealing. If in the evidence that you present to us you want to go into some of the detail of any amendments or drafting issues that you feel would improve the Bill, which you mentioned earlier, please feel free to do so and send those suggestions to us. Thank you very much for coming along today.