HOUSES OF PARLIAMENT

Joint Committee on the Draft Investigatory Powers Bill

Oral evidence: Draft Investigatory Powers Bill, HC 651

Monday 21 December 2015

Watch the meeting

Members present: Lord Murphy of Torfaen (Chairman), Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Hart of Chilton, and Lord Strasburger

Questions 197 - 223

Witnesses: **Rachel Griffin**, Director, Suzy Lamplugh Trust, **Rachel Logan**, Law and Human Rights Programme Director, Amnesty International, and **Alan Wardle**, Head of Policy and Public Affairs, NSPCC, gave evidence.

Q197 The Chairman: A very warm welcome to all three of you. Thank you so much for coming along so close to Christmas. We are very grateful. As you probably know, the way the Committee operates is that we will ask you a number questions, which we hope will give you the opportunity to make whatever points you want. I will open by asking you a very general question and in each of your replies please feel free to make anything you like by way of an opening statement. What do you think of the draft Bill? Do you think it strikes the right balance between safeguarding our civil liberties and crime prevention? Perhaps we can start with you, Ms Griffin.

Rachel Griffin: I should start by saying that I am from the Suzy Lamplugh Trust. We run the National Stalking Helpline. A large proportion of the people who we help each year are affected by digitally-assisted stalking of some kind or another. The first thing to say about the draft Bill is that it is definitely necessary, from our point of view, for the police to have access to communications data to investigate many cases of stalking and cyberstalking. It is certainly necessary for the police to be able to access communications data to investigate and detect crimes. However, the point we want to make is that legislation should be only one part of a strategic plan to address digital offending. On a day-to-day basis we are finding that the police often do not make very good use of the legislation that they already have available to them. Our question would be whether a change in legislation would have an impact on the experience of victims on a day-to-day basis. On whether the Bill strikes the right balance between safeguarding and civil liberties, I defer to other organisations to answer that question. Our point of view is very much on the experience of victims of stalking.

The Chairman: That is what we would expect it to be.

Rachel Logan: Amnesty very much welcomes the opportunity to be here. We very much welcome having a draft Bill of some kind, because we are one of those organisations that has been saying for a long time that the existing statutory framework in this area is not up to scratch. Unfortunately, we are very disappointed by what we see in the Bill that has been put forward. To touch on a very small number of areas, given the time available, first, we see in the Bill not one, not two, but five sections dealing with bulk, indiscriminate collection of or interference with individual privacy. From our perspective, that simply does not strike the balance or draw the line in the right place. We even see some targeted powers shading into what we would see as bulk powers in the case of thematic warrants.

I move on to intelligence sharing, which we have been litigating on for more than 18 months in the Investigatory Powers Tribunal. It has been the subject of at least two rulings. We were very surprised to see in what bare terms it is dealt with in the Bill, given how big the subject area is. We would have liked to have seen a clear, accessible framework, dealing with how material is received and sent overseas outside the MLATs. We would have liked to have seen that limit and not include the product of bulk interception either way—going from the UK or coming into the UK.

On oversight and judicial authorisation, unfortunately, we are disappointed by the judicial authorisation, or judicial review process, as it is put in the draft Bill. It does not amount to proper, independent judicial authorisation as is required for human rights compliance. It is simply not there. On the oversight provisions, similarly, having been through the IPT—I hope that I will get the opportunity to expand on this—we are very disappointed to see only one real substantive change to the way the Investigatory Powers Tribunal does its job. We would have liked to have seen a much more thorough look at how that works and whether it is properly independent and effective.

Finally, to touch on special protections in the Bill, again, this is an area that Amnesty has been litigating on in terms of legal professional privilege in the Investigatory Powers Tribunal, where we saw a concession by the Government that their entire regime in this area had not been human rights compliant. We saw a further finding that one of our co-claimants' legally professionally privileged material had been unlawfully retained. It is very disappointing to see nothing on the face of the Bill to deal with that properly, to deal with journalists, or even to consider giving further protections to human rights NGOs, such as ourselves, who we now know have, disappointingly, been specifically targeted for surveillance by the state. With all of that in mind, and there are many other areas that we simply do not have time to get into at this stage with the time allowed for the Bill process, we are very disappointed with what we have been presented with.

The Chairman: Thank you very much. Of course, every organisation, including yours, is very much entitled and welcomed by us to submit written evidence in detail.

Rachel Logan: We have done, this morning, for which we are grateful.

Alan Wardle: Good afternoon. Another fact that is relevant for this is that the NSPCC runs ChildLine, which you will all be aware of. It is now in its 30th year. Increasingly, children, as the Committee will know, are leading their lives online. More than three-quarters of 12 to 15 year-olds have access to a smartphone. That also means that many of the crimes

committed against children increasingly have an online element. In particular, some of the ones I want to focus on are what you might call the harder-end cases, such as the possession, distribution and manufacturing of child abuse images, so-called child pornography, which is growing, and also cases of grooming of children, much of which is done online. More than 500 children contacted ChildLine last year about grooming and more than 80% of those cases had an online element to it.

From our perspective on the Bill, the most important thing for us is to ensure that the police have the powers that they need to track, investigate and prosecute these offenders. We are coming from a different place from Amnesty, which is more about bulk surveillance; we are more focused on specific criminal investigations that the police need to undertake. We have a particular concern that Clause 47 might be restricting too much the police's ability to investigate in what can be quite complex investigations.

Another point I want to make is that ChildLine has a very high level of confidentiality, but it has to breach children's confidentiality around 10 times a day, generally because those children are actively suicidal. Most children contact ChildLine online these days, so we need to ensure police can get those IP addresses quickly and actively intervene to protect those children. The two aspects that I would like to talk about are criminal investigations and ensuring police have powers, and an emergency function to protect a child's life if they are in immediate danger.

The Chairman: Thank you, all three of you, very much indeed for those opening remarks.

Q198 Mr David Hanson: The police's case, as put to us by Keith Bristow of the National Crime Agency, is that the Bill brings us up to speed with "what we need to be able to do in a digital age compared to an analogue age". Do you agree with that, or do you think the Bill goes further and adds new powers for the police?

Rachel Griffin: I smiled because I can see why that statement was made in theory, and it might well apply to cases of, for example, child sexual exploitation, where the focus is on intervention and stopping criminal activity escalating. From a stalking point of view, the key use of communications data in cases that we deal with is on investigation and detection in individual cases where the activity has already happened. We tend to find that it is not so much a case of whether the police have the powers; they already have a number of powers but we find that they simply are not being used in practice. For example, we often hear from victims of stalking who have been told to turn off their computer—"If you don't look at the emails it won't affect you"—or they might be told that that it is too expensive to investigate digitally, or that there is no point as the service providers will not be compliant, et cetera. For example, recently the helpline report was told that police access phone records only in cases of murder. There is a huge gap between what is going on in practice with regard to making use of existing powers and what may be envisaged in terms of the potential of the Bill. That is why we would like to see the police using their current powers to full capacity, as is reasonable and proportionate, but also to focus on not just legislation but the capability and capacity of police forces to make use of that legislation.

Rachel Logan: I will leave this to my colleagues at this stage.

Alan Wardle: The police's view on powers is quite important. From our perspective, we understand from the NCA that there has been a gradual erosion of the amount of data that they have been able to gather over the years. The Bill is very important to put that in place and to ensure that it is adaptable. Who knows what technologies there will be in five to 10 years' time, but the Bill has to have sufficient flexibility to adapt to those things.

On Clause 47(4), which has additional restrictions on granting authorisation, we have had initial conversations with the police and they have expressed concern about it. It would seem to us perverse if the data providers were able to hold all the information but the police were unable to access it. My understanding is that if people were conspiring over the telephone the police would be able to have all that information, but not if it was done online. That subsection talks about where the activity is mainly or wholly acquiring material the possession of which is a crime. Something such as possessing child abuse images is clearly a crime, but we know that for grooming cases where a lot of people are involved and it takes a long period of time, where, for example, a person books a hire car in place A and drives to place B or they book a flight, those factual issues, while not a crime in themselves, can help the police to investigate. It would be worrying to us if anything restricted the police's ability to investigate thoroughly along all the different strands of investigations. We would want to ensure that there is parity across the board and that the data the providers hold can be accessed by the police force for specific investigations.

Mr David Hanson: The question to all of you is: are the police powers under existing legislation proportionate and effective? Will they be more proportionate and effective under the proposed Bill, or will they be neutral or less effective? What is your view as to the police-central cases: do we need the Bill to update what we currently do? Is that right?

Alan Wardle: Yes it is, but my understanding is that this clause in particular would place a restriction on them that is not currently there. That would need to be worked through to see why it has been put in there and whether it will actively hinder the police's investigation of the kind of complex cases that I am talking about: the production of child abuse images, which, again, are quite often done by conspiracies, and online grooming. Yes, the need to have these additional powers is quite clear.

Rachel Logan: I am afraid that the question of police powers is not something that Amnesty can assist the Committee with at this point. It is not a part of the Bill that we have assessed or been involved with to date.

Mr David Hanson: With due respect I think that that is copping out of an answer. If the Bill goes forward, is Amnesty satisfied that the current proposals by the police are modernising their view based on the Bill? Ultimately it is about police powers and whether they are effective and proportionate. Surely Amnesty has a view on that.

Rachel Logan: With respect, it may be seen as copping out, but we are talking about a Bill of many hundreds of pages and many parts. Amnesty is a worldwide movement that focuses on many different aspects. We simply have not assessed those parts of the Bill yet.

Mr David Hanson: So you do not have a view on whether these current proposals are proportionate and effective.

Rachel Logan: At this point I do not have a view that I can assist the Committee with on the police powers in those parts of the Bill. I can help you, as much as Amnesty can, with questions of necessity and proportionality around bulk interception warrants, the structures around targeted warrants, and what is in the Bill on intelligence sharing, but I am afraid that the question of police powers and dealing with crime simply is not something I can help you with.

Mr David Hanson: Ultimately those are police powers. The question is whether they are proportionate and effective in relation to what the Bill proposes.

Rachel Logan: I am afraid that this simply is not something that we can assist you with. Those parts of the Bill go into Parts 3, 4 and 5. There are multiple parts of the Bill. We have not had a significant amount of time and they are not core areas of focus for us at this point.

Mr David Hanson: May I respectfully suggest that, when the Bill comes before both Houses of Parliament we would want a view on those issues? They are central to the Bill.

Rachel Logan: It may well be that, when we have had considerably more time and when the Bill goes through the proper processes, we will turn to that. I simply cannot say at this stage whether that will be Amnesty's focus.

Rachel Griffin: Our view is that it is unlikely—or that we are yet to be convinced—that the Bill will have an impact on the majority of cases of stalking as we experience them. That is not because data communications are not needed, but because the expertise in digital investigation and recognising risk is not as widespread in day-to-day policing as it needs to be.

Q199 Suella Fernandes: This is a question to Rachel Griffin and Alan. Can you walk us through a typical harassment case—if there is such a thing—or a child sexual exploitation or a grooming case, and how communications data would be helpful in identifying perpetrators and securing a conviction?

Rachel Griffin: From a stalking point of view, around 70% of people who call the National Stalking Helpline report experiencing at least one form of stalking behaviour that may require police to access some kind of communications data. Some 39% have received phone calls; 30% have received emails; 36% have received texts; and 37% have experienced stalking via some kind of social networking site. It is right that you made the point that there may not be a typical case of stalking because each one would be quite different. They are incredibly diverse in how long the stalking goes on for; some will be stalked for about six months, but, sadly, we have a small proportion of people who have been stalked for a number of years.

What tends to happen is that somebody will be stalked through a blend of different means. That may include physically turning up at someone's workplace or at their home, perhaps sending them letters, but also saying things about them via social media. Some will know that they are being stalked and that the activity is taking place online, but they do not necessarily know who it is, or there is a suspect but it is very difficult for them to prove. They will go to the police and say, "This has been happening, I've been receiving these text messages, these things have been written about me on Twitter". In a case where there

may have been a number of text messages or emails, the police may need to identify that it was in fact a perpetrator—an identified individual—who sent them. That is where communications data may come in. Unfortunately, that is where we have too many examples of victims saying that they have gone to the police and found that, in some cases, the police do not even understand what an IP address is. The level of understanding is relatively low. That is alongside those cases where people say, "Well, come back when he does something", suggesting that if it happens on the internet—if the stalking is cyberstalking—it is not real stalking.

Alan Wardle: It varies in grooming. Sometimes it can be one person grooming one child, or, as we have seen in some high-profile cases, it can be gangs of people communicating with several children. The process of grooming takes time, by its very nature. It lures children in, makes them feel good about themselves, offers them enticements, et cetera. We know from the National Crime Agency that the vast majority of cases involving grooming are online. That could be through social media, by various apps, by text message, by phone et cetera. Quite often, one of the challenging things around this is that children do not even recognise that they are being groomed—they think that it is their boyfriend, for example. The child will not necessarily keep the evidence themselves; they will not hold on to it. The police need to be able to identify from all those different sources what happened, to try to get a picture of who said what to who, where they were, who they communicated with, when they did it, et cetera, to build up a picture of what is going on, which obviously would go alongside personal testimony. That is why the point that Rachel Griffin makes is valid: we also have concerns about the police's capability—particularly that of local forces—to investigate and understand these offences properly. The cornerstone to that is having the information available to them so that they can identify what has happened, build up a picture of what is going on and investigate and prosecute these crimes.

Q200 Baroness Browning: Are the three purposes for which law enforcement can seek internet communication records the right ones? Should they also be able to use them for other purposes—for instance to locate missing people—even when no crime is suspected? We have received evidence from the police that much of their time is taken up with trying to identify vulnerable people, not necessarily because they have fallen foul of serious crime, but speed is of the essence because they are vulnerable.

Alan Wardle: On the first part of your question, as I mentioned, certainly on Clause 47(4)(c), which is the limitation where a person is "making available, or acquiring, material whose possession is a crime"; at first glance, and having had an initial discussion with the NCA, we are concerned that that might be too limiting. Using grooming as an example again, hiring a car to transport a child from one part of the country to another is not a crime in and of itself, but it is evidence of a crime having taken place. It would be worrying to us if that data was held by internet service providers but the police could not access it because it was not illegal material. More needs to be teased out throughout the process about what that means and what limitations that will place on the police.

On the emergency bit, as I said, ChildLine has to do this about 10 times a day. We work with CEOP very closely. The ability of the police to identify and rescue actively suicidal children who may not want to be contacted by the police is a very important function. We certainly would want to ensure that that capability is not eroded in any way.

Baroness Browning: Not eroded, but as drafted, will it not add anything to resolve the problem of your 10 children a day?

Alan Wardle: I spoke to a barrister about this last week. Her initial view was that Clause 46(7)(g), "for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health", would cover this situation, but again, it would be useful for the Home Office to clarify whether, in its view, that would cover it.

Q201 Lord Strasburger: Ms Logan, you mentioned in your opening remarks that one of the five areas you are concerned about is intelligence sharing. There is very little in the Bill about it and so far the Committee has heard very little about it. Would you care to expand on what Amnesty's concerns are and what advice you would give the Committee on it?

Rachel Logan: Yes, thank you very much. Amnesty has been engaged, together with Liberty, Privacy International and several other NGOs, in litigation in the Investigatory Powers Tribunal—it will now be off in the European Court of Human Rights in Strasbourg on this subject—to look at the way the UK both sends information, intelligence product, overseas and receives it from overseas powers. In the Bill we have very little at all on what are called "overseas arrangements". Clause 39, "Interception in accordance with overseas requests", provides for that activity, but simply talks about lawful interception being something, "carried out in response to a request made in accordance with a relevant international agreement by the competent authorities of a country or territory outside the United Kingdom". The only definition you have for a "relevant international agreement" is, "an international agreement to which the United Kingdom is a party". On the other side of the coin, when we think about what the UK is requesting others to do—perhaps not requesting, but what information it might receive from other powers—all we have in the Bill is a bare reference in Schedule 6 to a "code of practice", which, it is said, will be forthcoming and which will deal with the "provision about the making of requests ('relevant overseas requests') for intercepted material or related communications data that has been obtained by an overseas authority by means of any interception", et cetera, with no definitions of what any of this might be and no expansion on what any of this might mean. There is then further provision for arrangements to be in place around receipt or sending of such information, with no explanation of whether such arrangements will be public, what they might contain or what they might be.

We were talking about the product of bulk interception, such as, in the US, the product of Prism or the upstream programmes where material has been collected in bulk. We are considering a situation where we have a ruling in the Investigatory Powers Tribunal case that recognises that, until this litigation, any such intelligence sharing was unlawful because there was no policy whatsoever in the public eye in this area. All we got during the litigation was a small summary, which was corrected on many occasions, of what the arrangements in place might be. It was very bare bones. There was lots of talk about signposting to what was under the waterline. When we were in that situation we had very much expected the Bill, in the spirit of transparency, to provide a clear legal framework. Those simple references simply do not do that. How can Parliament and the oversight bodies provide proper scrutiny? How can the public understand where their information might end up or what might be being looked at overseas if there is simply nothing there? That is very disappointing.

The Chairman: I think we will touch on that in further questions as well.

Q202 Dr Andrew Murrison: Amnesty obviously has an international perspective. I am interested in your view on whether this legislation is compatible with the direction of travel taken by countries with which we can reasonably be compared, in particular the other four members of the "Five Eyes" community.

Rachel Logan: I want to be very careful about what I say on that topic at this point because there is a certain state of flux in the relevant "Five Eyes" countries. I would be very happy to come back to the Committee with a more detailed analysis. I will say that in the US, for example, we have recently seen, as I am sure you are aware, changes around the Patriot Act and the Freedom Act and a certain amount of rolling back, but I would not want to give the Committee any precise answers without being able to go back to that in more detail. I would be happy to do so.

Dr Andrew Murrison: It would be quite valuable if you could as part of written evidence. As we have been going through this there have been comparisons with the "Five Eyes" community, with whom, of course, we share data. It would be useful from your perspective as an international organisation to provide some insights if you could.

Rachel Logan: I will certainly see whether we can do that in the time available.

Dr Andrew Murrison: Thank you very much. May I ask you about communications data? A lot of what we have been dealing with over the past few weeks has to do with the times permitted by the Bill—for example, five days for judicial review warrants issued by the Home Secretary and 12 months for the retention of communications data. I would be interested in your thoughts on whether 12 months is right—in particular, to nuance that slightly, whether that 12 months might be amended upwards or downwards depending on the situation, on the crime that we think has been committed and on the circumstances, thinking of missing people, for example.

Rachel Griffin: We would resist offering an arbitrary time limit, which I dare say is not terribly helpful. From the National Stalking Helpline's perspective, we tend to talk to people at the very beginning of their journey through the criminal justice system. They may not even have reported the crime when they talk to us. I would advise getting evidence from people such as the CPS and the police on how long it takes for a prosecution to come to court from that point of first report. That will have an impact. It will not be terribly helpful to have a time limit that may have expired when the evidence is finally gathered and a prosecution is pursued.

Also, it is worth bearing in mind how long people have been stalked for. Some 48% of the people who talked to us have been stalked for longer than one year. That suggests that there might be a need, by the time a victim goes to the police, to go back some time to find some of the essential data. It is also really important to understand why people do not come forward, whether it is to do with cyberstalking, or, in the context of stalking, things such as revenge porn. Often people will not come forward because they do not feel that they will believed and they do not have the confidence to talk about their experiences.

Also, it is vital to point out that, in preparation for this session, we contacted the Home Office to ask how many investigations are impacted by lack of communications data—we

do not know what we do not know. The feedback was that it is impossible to know how many criminal investigations are impacted by a lack of available communications data. Again, I come back to the point that we definitely recognise the need for communications data, but we do not know the size of the problem that we are trying to solve with the Bill. Therefore, it is difficult to determine whether the existence of the data would be helpful and for how long that data would need to be kept because we do not know how many prosecutions are not going forward without that data. It feels very circular.

Dr Andrew Murrison: Where do you think the Home Office got the figure of 12 months from, then?

Rachel Griffin: I am not sure. You would have to ask the Home Office.

Alan Wardle: My understanding of the 12 months was that the last time this was legislated for Parliament took the view that that was the appropriate time. Any flexibility around that ought to be evidence-led. Certainly, we know that some of the more complex cases, some of which I have alluded to, take a long time to build up the case. We hear from the police of cases where, because it is a rigid 12 months, as the case proceeds bits of evidence fall off the end after a year. We need to know whether there is any flexibility around that once a case has started. On disclosure, again, similar to the point that Rachel made, not all children disclose immediately whether they have been abused. They can take time. It is a judgment for Parliament to make. It ought to be evidence-led and take a view on whether there are more serious and complex crimes where data need to be held for longer and how that would work.

Dr Andrew Murrison: I can see why organisations such as Suzy Lamplugh Trust and the NSPCC should want the police to have these powers since you are faced, on a day-to-day basis, with very vulnerable people. However, do you have any concerns more broadly about the acquisition and storage of communications data and potential misuse of that material?

Alan Wardle: Yes. It clearly needs to be kept safe. Another thing to remember is that children are users of data as well and they will want to have their rights and privileges protected. Clearly, there have to be very strong safeguards around that. I am not a technical expert so I would not be able to tell you how that is done, but the data needs to be kept securely. It needs to be accessed in very strict conditions to give people confidence and assurance that the data is being used properly.

Rachel Griffin: I echo that. There will be a number of cases where someone who has been stalked will have their security, whether physical or online, compromised in some way. It is critical that they have confidence that their data will be treated appropriately.

Dr Andrew Murrison: In situations such as that of TalkTalk, are you confident that there are likely to be systems in place to guarantee people's safety and security?

Rachel Griffin: Guaranteeing safety and security is very difficult. It is particularly difficult when someone is motivated by the kind of obsession and fixation that stalkers commonly display. It would be completely wrong for me to say that I would have confidence that that can be guaranteed, but victims should have a reasonable expectation that their data will be kept as securely as possible.

Q203 Lord Hart of Chilton: I must disclose to the record that 50 years ago at university I joined Amnesty International.

The Chairman: You have disclosed your age as well.

Lord Hart of Chilton: I know—how youthful I still look. We have been supplied with the open determination of the Investigatory Powers Tribunal on 22 June 2015, from which we see that GCHQ retained material for longer than permitted under the policies. Therefore, there was a breach. My first question is whether, in the light of that decision, you are confident that there are sufficient safeguards in place governing the activities of the intelligence and security agencies. I rather think from what you said at the opening that you are not.

Rachel Logan: No, indeed. First, it is important to think about what that finding tells us and then look at whether we feel that the safeguards are sufficient in the light of that. It is important to understand that Amnesty found very little out from that determination. I can come back to the question of how we got it, which sheds rather a lot of light on our views on the Investigatory Powers Tribunal, but it tells us very little at all. We do not know why our communications were intercepted and selected for examination. We do not know what was looked at and when. We do not know what policy was breached or in what way. We do not know whether this was a one-off and just confined to us, or whether it is systemic among other NGOs that were not involved in the litigation. We have had no ability whatsoever to input into the conclusions of the tribunal because we were excluded from the hearing that resulted in that determination. That begs the much more important question, as far as we are concerned, which is why human rights NGOs were being targeted for surveillance in the first place, quite aside from whether our material was retained for too long. The other NGOs in the same legal action received a simple one line, "No determination in your favour", which does not tell them whether they were intercepted, or whether they were intercepted but the tribunal considered it to be lawful, et cetera.

It is a very sparse determination, but what that tells us about the safeguards and the oversight system is that something has gone very badly wrong. It appears that this has been considered an acceptable activity by the Secretary of State and all those others involved in oversight during the process, because we know that we were picked up under a general warrant. It appears that this is something that was carrying on which either nobody raised any objection to because they all thought it was fine and dandy to be spying on human rights NGOs and did not know about the specific policy breach, or they knew about the breach and did not consider it to be important. We do not know why this was not picked up until we got into a tribunal process. It is very worrying that we had to get to that stage to get this finding.

The same applies to the other litigation we have been involved in—the legal professional privilege one I alluded to earlier—where one of our co-claimants found that his legally privileged communications had been picked up. That is a really frightening proposition for those of us who have been involved in the legal system for a long time. Again, he was not able to contribute to the hearing where the finding was made that this was not very important. From our perspective, something needed to change with that in mind. We have not seen that something in the draft Bill, particularly if you look at the retention provisions

in it. Data can be retained as long as it is necessary or "likely to become necessary" to retain it. That is stunningly broad. It is very worrying for us, having been in the position of having had our data retained and having been spied on, that we do not have more safeguards in this. I can come on to look at the IPT and the judicial relation if you would find it helpful, but basically, against that background, there does not seem to be enough.

Lord Hart of Chilton: What further safeguards do you think are necessary?

Rachel Logan: It comes back to the question of definitions. There are incredibly broad definitions around purposes in the various warrants. There is no definition of national security. Just recently, a decision by the Grand Chamber in Strasbourg, I think last week, said that it is important to have tighter definitions than just "threats to national security" when we talk about warrants of this kind. You have these very broad definitions and general purposes permitted as a basis of interception. Then you again have a complete absence of proper judicial authorisation. In Amnesty's view, this so-called double lock does not amount to a human-rights-compatible process. The decision is still being taken by the Secretary of State. It is merely being reviewed on judicial review principles by a judicial commissioner. If Clause 19(2), which states that this must be done to a judicial review standard, was not intended in any way to limit the scope of the review undertaken by the judicial commissioner, then it is unnecessary or unnecessarily complicating the situation.

Our view—like, I am sure, many of the other NGOs you have heard or will hear from—is that that is simply unnecessary if the intent is to have a full, merits-based review by an independent judicial authority before a warrant can be issued. We would like to see that happen. We would like to see strong post facto oversight done by different people than those involved in the authorisation process. This melding of the oversight and authorisation functions with the judicial commissioner is something that worries us. Down the line, looking at the Investigatory Powers Tribunal itself, I have spent nearly two years now litigating in this tribunal alongside some very well-known QCs from my old chambers and elsewhere who are well-versed in SIAC and other places where there are secret processes and unusual court systems. This court and these processes are the most frustrating and obfuscating that I have ever encountered in the UK system. We are talking about situations where, whether for intent or not—I am sure not, because everyone wishes this to be open—the bias is towards secrecy and not letting the claimant in to what is ultimately a determination of their rights and freedoms. That needs to change. All we have here is an additional right of appeal. There has been no further look at the procedures of the IPT, which allowed the Government to argue this year that, even if the tribunal made a determination to favour individuals—that they said behind closed doors, "This person's rights have been violated"—they should not have to tell the claimant. They could lie and still say, "No determination in your favour". We had a whole hearing on that topic. In the end the tribunal rejected it, but there is that level of vagueness and secrecy in the tribunal's rules. That simply has no place in a rights-compliant oversight and authorisation system.

Lord Hart of Chilton: Do you think, then, that there should be a blanket exemption for legally privileged communications?

Rachel Logan: That is the basis in English law. This is not a question merely of human rights law, this is about the common law.

Lord Hart of Chilton: No, but in respect of this Act.

Rachel Logan: Yes, we do. All there is here is a provision for codes to be available. We have to look at the safety of the justice system, as well as rights and freedoms. This is the most sensitive and the most basic principle. If I cannot, as a lawyer, say to my client that what they are telling me is entirely confidential, how can I know that they will feel free and safe and able to give me full information? There is a significant chilling effect from the mere fact of interception of legally privileged communications that really needs to be taken into consideration.

Lord Hart of Chilton: You mentioned a moment ago the Investigatory Powers Tribunal. Do you think that the provisions there are satisfactory? Again, I rather gather that you do not and that you do not think that the Investigatory Powers Tribunal provides a satisfactory route for appeal and remedy.

Rachel Logan: Indeed. The judgment we received from the Investigatory Powers Tribunal on 22 June was not in fact the final judgment in that hearing. The judgment on 22 June said, "There has been no determination in favour of Amnesty International; that is, you have not been unlawfully intercepted. There has, however, been a determination in favour of the Legal Resource Centre in South Africa—a very well-respected NGO—and the Egyptian Initiative for Personal Rights". On 1 July, having had a period for corrections and clarifications to the draft judgment, none of which were put into effect by the Government, we received an email out of the blue from the Investigatory Powers Tribunal informing us that there had been a mistake and where the judgment said EIPR, it meant Amnesty International. That was following a hearing that supposedly was looking in the most detailed consideration at our rights and at particular communications that had been intercepted and whether that was lawful and proportionate. We asked, quite rightly, "How can this happen?", and asked for an open determination explaining how a mistake of this kind had been made. We received a very unsatisfactory response from the tribunal. Indeed, Parliamentary Questions have been asked about this by quite a few Members of the House—both Houses, in fact—seeking a Statement from the Secretary of State, asking whether other human rights organisations have been in the same position, and nothing has been forthcoming. That casts light on quite how problematic the IPT currently is. It needs to be sorted out.

When it comes to the Investigatory Powers Commissioner, we set out in our written submission that it is mostly things around the edges, around independence and effectiveness. We would like to see the oversight and authorisation functions separated. This is a small group of people and they will be looking at the full process to see if it has been gone through appropriately, and reviewing that. In our view, it would be safer to separate out the functions of overseeing the process and undertaking the process, even if it is just a part of it.

Q204 Matt Warman: I would like to ask a supplementary question. Were you saying that there would be a chilling effect if legally privileged communications were intercepted? As I understand it, that power has already been avowed and therefore theoretically it is already happening and lawyers and their clients might reasonably worry about it. Has there been a chilling effect, given that this is something that could theoretically happen already?

Rachel Logan: I cannot speak for the entirety of the legal profession, I am afraid, I am simply one representative of it—and from Amnesty, obviously. It has certainly caused enormous concern to us in how we deal with our clients. Amnesty does worldwide research and litigation on a range of human rights issues, often right at the edge of the issues that Governments are uncomfortable with; for example, looking at the involvement of our own Government in rendition and abuses during the war on terror. But we are also very much concerned with Governments overseas. It is very difficult for someone intercepting our material under a broad warrant to distinguish between what might be country research material and what might be professionally privileged because it concerns witness statements, instruction, et cetera. We are very concerned about the impact of knowing that material which is legally and professionally privileged is being picked up in their net.

Matt Warman: So has it had a chilling effect on your own communications?

Rachel Logan: I am not quite sure what you mean by that. Are we extremely concerned and worried about what we say? Yes, we are.

Matt Warman: Has that changed since the power was avowed in this country?

Rachel Logan: There is always a difference between when you worry that something is happening and when you are told that it actually is happening so, to that extent, yes.

Matt Warman: Moving on to communications services providers, from an NSPCC perspective, are you worried that communications service providers co-operate sufficiently at the moment, when information could help the kind of work that you do?

Alan Wardle: Generally, things are pretty good. Looking at issues particularly of child abuse images and how those are disseminated across the internet, Google and Microsoft—at the instigation of the Prime Minister—did some really good work a couple of years ago which means that it is much more difficult to find those images through an open search on the web. Now, with some 100,000 search terms, you get only what are called clean searches; that is, they do not give those images. So that has been good. Most of the big companies are involved with the Internet Watch Foundation. Certainly in this country we are pretty proactive so if an image is found, it is generally down within two hours, so that is pretty good.

On the content, because the majority of the big companies are American, you would have to ask the police. I am not sure how the investigation of the content of communications is working. We have an issue with some of the internet hosting companies, such as online storage functions where people are uploading and storing a whole host of images. We think that that issue needs to be looked at in more detail and we are looking at it at the moment. Most of the companies recognise that this is a very serious issue and they are generally very co-operative. It is a global issue so, while the UK is very seized of this issue, we are seeing some alarming developments in other parts of the world—such as livestreaming of child abuse, which is crowdfunded—which is why these sorts of powers are essential.

Matt Warman: Will the Bill improve that situation or not make that much of a difference?

Alan Wardle: Internet connection records are very important, as I have already indicated. When it comes to the information that is needed, the current process is often very convoluted, when you have to go through the MLAT process. Anything that could be done to simplify and expedite that would be good. We know from the police that they do not even bother to apply for evidence in some cases because they know it will take too long.

Rachel Griffin: We have had feedback from police officers we have worked with on the National Stalking Helpline that communications service providers are not always helpful in cases where the police need their assistance. But we do not really know whether this unhelpfulness is to do with reluctance to help, misunderstanding of what help is needed, or because the legislation needs to change. What is clear is that CSPs, as well as improving co-operation with law enforcement agencies, need to provide more assistance to the victims, who are often seeking help, advice and protection after being targeted when using their services. Again, it is very difficult to say whether the proposals in the draft Bill will improve that co-operation without having a better understanding of what the barriers are perceived to be by the CSPs themselves.

Q205 Suella Fernandes: I have a follow-up question for Amnesty. You talked a lot about privacy rights. Obviously, we have to strike the right balance but I heard very little about national security. We have heard a lot of evidence and we have on the public record that the head of MI5 has said that we face an "unprecedented scale and character" of terror threat at the moment. We have heard from witnesses about very serious crimes that are being perpetrated online. You obviously do not feel that the draft Bill is satisfactory but where do you think the balance should be struck in meeting this very important need to safeguard the public?

Rachel Logan: There is of course a critically important need to safeguard the public. That is part of human rights protection and we all have the right to life and security and all those sorts of things. That is part of what we are looking for as an organisation. But as you say, it is a question of proportionality and where you draw the line. For example, I am sure that it would be useful for crime prevention and national security purposes if we all had to go round with a body camera on, videoing where we were at all times, and had to hand that tape over at the end of the day, or if we had to keep a list of everywhere we went and everyone we spoke to, and handed that over. That might well assist in preventing more crimes, but for most people that would be an intolerable level of intrusion into their private lives. For us, the Bill simply does not draw that line in the right place. Targeted, suspicion-based surveillance is a very different world from what is being proposed here.

Suella Fernandes: When it is necessary and proportionate.

Rachel Logan: This is the question. "Necessary and proportionate" usually means the least intrusive measure that can be used to achieve a legitimate aim. That is precisely the question that we are all here to debate and we do not think that the Bill has that line in the right place.

Suella Fernandes: My question to you, Rachel and Alan, is this. The Anderson review described Tor as a facility that enabled the digital abuse of anonymous activism and dissident activity. What is your view of this Bill's potential effect on encrypted communications in the context of your work?

Rachel Griffin: I would certainly refer you to those with greater expertise than me on the digital side of things, but my observation about encryption is that stalkers and cyberstalkers are fixated individuals who will use any means available to them. We have had a number of cases where victims of cyberstalking have had their devices hacked by stalkers, and in those cases we have advised them to use encrypted services in future. We have experience of encryption being used for both good and bad reasons. Obviously a balance needs to be found, but I do not have the expertise in encryption to answer that question in an informed way.

Alan Wardle: Tor is a place where quite a lot of the most dedicated—if you can call them that—people who perpetrate these crimes go, particularly in the production and dissemination of child abuse images. Essentially it is a challenge for law enforcement. Being able to identify the perpetrators is very time-consuming, and I do not think that anything in the Bill will necessarily affect that. It is one of those things, given the way the internet is designed. A third of internet users across the world are children, but the internet was never designed as a child-friendly place, and we are almost going around saying, "Can you put safeguards in at the beginning?" Would you design it in this way now? I do not necessarily know that we would, but we are where we are, and certainly from our perspective the key thing, as well as power, is law enforcement dedicating the necessary resourcing and skills to get officers to do the quite painstaking work of cracking these rings of people, which are global and are perpetrating some of the vilest crimes against children. We need to ask encryption experts about that, but it is certainly challenging for law enforcement and we need to make that it has the resources—the powers, the skills, the expertise—to be able to deal with these policing challenges in the 21st century.

Suella Fernandes: I have one last question on a point that both of you raised earlier. You mentioned suicidal children getting in touch with you as well as tracking and trying to pinpoint people who are involved in stalking. Can you give us an idea of the need for timeliness in securing warrants in those situations? When you are in the process of an investigation or trying to track someone down, do you operate in a series of days and months, or is it hours and minutes that you and the law enforcement services need in order to exercise your powers?

Alan Wardle: For ChildLine it is hours and minutes. Someone will be called at 4 o'clock in the morning to breach that child's confidentiality, if that is required. There are cases of the police literally cutting down children who are found hanging and saving their lives. I was in a meeting with one of my directors not so long ago. They had to authorise something; the police intervened to protect a child who was about to jump off Tower Bridge. In those cases, it is a matter of hours and minutes, which is why there is a need for the systems that we have in place in CEOP, which are very fast and rapid. If a ChildLine counsellor and their supervisor think that the child is in immediate danger, sometimes that speed is of the essence.

Rachel Griffin: This is an excellent question, because it really helps me to draw out the distinction, as I see it, between our perspective and an organisation that is working on child exploitation. Very rarely will we deal with a victim of stalking where there is not enough risk information for the police to put protection around that victim based on a fairly well-established stalking risk assessment protocol. It is very rare—I cannot think of an example—that the information to put that protection around that victim was dependent on accessing communications data. The communications data concerns on the part of the

victims we deal with come about when evidence is being gathered to support an investigation and prosecution retrospectively. Given where stalking tends to sit in the list of priorities in a number of police forces, particularly digital stalking, which is perceived as difficult to investigate, that is where victims of stalking will end up, I fear—often at the bottom of the list of priorities.

Q206 Lord Butler of Brockwell: My final question is to Ms Logan, if I may, following up Ms Fernandes's question. Is Amnesty International opposed to bulk interference per se?

Rachel Logan: It depends on how you think about that question. Do we think that bulk interception draws the right line in the sand? Do we think it is a proportionate way of dealing with the threat? No, we do not.

Lord Butler of Brockwell: So as things are, you do not agree with bulk interception at all.

Rachel Logan: As currently laid out in the Bill, we do not consider that bulk interception—indiscriminate, suspicionless surveillance—is proportionate interference into an individual's rights.

Lord Butler of Brockwell: What needs to be done to the Bill to make it acceptable to you?

Rachel Logan: I am afraid that I can only talk to the parts of the Bill that we have assessed so far. We would like to see the provisions on bulk interception warrants stripped out. We would also like to see a change to the section dealing with so-called targeted warrants, which provides for incredibly broad thematic warrants, changed and provided with much tighter definitions. We would like to see a return to suspicion-based interference, the suspicion-based surveillance of individuals who are properly identified and properly targeted, as we would do normally in normal, day-to-day real-world life.

The Chairman: Thank you, all three of you, very much indeed. It has been a fascinating session. Thanks for coming along, and happy Christmas to you.

Witnesses: **Professor Bill Buchanan**, Head, Centre for Distributed Computing, Networks and Security, Edinburgh Napier University, **Eric King**, Visiting Lecturer at Queen Mary, University of London, and **Erka Koivunen**, Cyber Security Adviser, F-Secure Corporation

Q207 The Chairman: A very warm welcome to all three of you. Particularly as we are so close to Christmas, it is very good of you to come along and give us the benefits of what I know is your considerable expertise, knowledge and experience. We very much look forward to listening to you. I will start by asking you a general question, which will give you the opportunity, if you so wish, to make any general statements about the Bill. Will it work? What are your views on the draft Bill from a technical standpoint and are these proposed powers workable? Perhaps we will start with Professor Buchanan.

Professor Bill Buchanan: Thank you. I would say that we live in a very different world from the one that we did. We have built this cyberage within about 40 years, but the infrastructure that we have created is very fragile. We must protect citizens from hackers and so on. We must protect privacy and identity. More and more services are moving towards the provision of both privacy and identity. Individuals need to be assured that they are not being spied on by cybercriminals across the world. They also need to be able to prove their own identity and the identity of what they are connecting to.

Encryption involves both these aspects. It keeps things private but it increasingly is also used for identity provision. Much of cryptography is now focused on proving the identity of the services that we connect to. Just now, most of the services that we use in the cloud—Google, Amazon, Facebook and so on—are encrypted. Every time we see "https" and we see a green bar on our browser, it means that we are protected with a unique cryptography key for every session that we create. It is almost impossible to crack that key without knowing the private key of the site to which we are connected. The only way that someone could crack communications through a tunnel such as that is to get the private key off the company that is involved in the communications, which would involve Microsoft, Facebook, Twitter and so on handing over their private keys. The problem around that is that if someone gets access to those private keys—those special keys—we open up the whole of the internet and we will have the largest data breach that has ever been caused.

The communications that we have are obviously highly sensitive. The logs that we see on the internet are really the history of our whole lives. They are our thoughts, beliefs and dreams almost by the second. Every single thing that we do is recorded in our web history. The amount of money that that would be worth to a criminal—a cyberhacker on the internet—would be almost unlimited. If an ISP was hacked, you can imagine what the logs could be used for and what bribery there could be for individuals and companies. A balance needs to be struck between the privacy of individuals, the protection of our businesses and the risk of serious organised crime.

Erka Koivunen: Lord Chairman, it is an honour to be present in this Committee session. It has been a fascinating journey to read through the Bill, in particular as a non-native speaker—it has been a tedious task. However, I would like to offer my congratulations. The Bill is pretty transparent in the way in which it lays out the intentions of the Government to do a lot in terms of law enforcement and signals intelligence. This is a Bill

that you would get if you asked signals intelligence organisations what they would like as a Christmas present; they would reply that they wanted this and wanted it in bulk.

However, there are some unintended consequences when writing broad legislation that would give such exceptional powers to intelligence agencies and law enforcement. If there ever was a question whether nation states, Governments and military organisations would be engaging in hacking and computer intrusions, I guess that this Bill solidly sates that, yes, this is what they do and this is what the UK Government are actively seeking to do. Frankly, this is something that has been going on for quite a while now. The Bill is an attempt to put the existing situation in writing. We, as a provider of cybersecurity services to private companies and Governments, would typically advise our customers to be aware of criminal activity taking place and of their organisations being targeted by nation states and Governments as well. No better marketing material for services such as those that we provide could be envisaged. We should be aware that the powers laid out in the Bill could be misused. This will lead other nation states to try to mimic these powers. As a member of the European Union—I come from Finland, I am a Finnish national and our company comes from Finland—I feel that I am now a target of many of the activities laid out in the Bill. I do not think that this is what I signed up to when I joined up the cybersecurity profession. There are lots of discussions on how to limit those powers. I am not a lawyer or a legal person, but there are lots of things I can imagine technically that would undermine our society's security. Some of the things that we build in our online systems depend on strong cryptography, in terms of encryption, authentication and authenticity.

The Chairman: Thank you so much indeed. It is very good in English and in Finnish. Mr King?

Eric King: I will not repeat any of the feelings and concerns that both Bill and Erka have highlighted, but perhaps I can help the Committee in one regard by focusing your minds not on the question of whether the proposed powers are necessarily workable, because the majority of them are in fact already in use. That is not to say that they are powers granted by Parliament—indeed, I would expressly say that that is not the case—but they are powers that our agencies have been deploying for a number of years.

It has only been this year for the most part that the public have found out about these and that they have been officially avowed. It was in February this year that the Government avowed hacking for the first time—it is now called "equipment interference". In the Investigatory Powers Tribunal a few weeks ago, I heard from government lawyers that bulk equipment interference apparently had still not been avowed. Bulk interception was only avowed with the writing of the ISC's report in March this year, for which we are very grateful. The use of bulk personal data sets, as mentioned in the Bill, were again revealed to the public only with the ISC's report in March. The ISC stated at the time: "Until the publication of this Report, the capability was not publicly acknowledged, and there had been no public or Parliamentary consideration". Bulk communications data acquisition was only avowed on the very day that this Bill was introduced to Parliament by the Home Secretary, who admitted that our Security Service, MI5, had been acquiring in bulk the phone records of everyone in the United Kingdom. Anderson commented at the time to the BBC that the legal power that had been relied on to exercise that authority was so broad and the information surrounding it so slight that nobody knew that it was happening.

I make these points to say that the Government, in my mind, should make operational cases from first principles for every single one of these powers. Simply because they have already been in use and simply because the agencies have interpreted law in a manner that they feel has made them lawful does not make them lawful. It is right that Parliament should receive a full operational case for each and every one of these powers. It is a matter of assessing not whether they are merely helpful or offer some form of value, but whether, given the scope of everyone's lives that they touch—after all, that is what bulk powers do—they can be vetted and scrutinised to make sure that they are both necessary and proportionate.

The Chairman: Thank you all three very much indeed.

Q208 Shabana Mahmood: I want to ask you about future-proofing the Bill. When the police, Home Office and others gave evidence to us, they were pretty robust in their view that these powers were sufficiently future-proofed against behavioural and technological change, as the powers were broad and wide-ranging. Other experts, in evidence, scoffed at the very idea of future-proofing, because of the pace of change in technology and how that impacts on behaviour in the online and digital space. What are your views on whether future-proofing is possible and, if so, whether that has been achieved in the draft Bill?

Professor Bill Buchanan: If there is one change that is happening in systems just now, it is a move towards the cloud. So like it or not, most of our emails are stored in the cloud, possibly in other jurisdictions. The main moves are with tunnelled web access. If someone uses a tunnelled connection, you cannot see the detail of the information that is passed. The minute someone uses https there is no way that you can see what page they accessed on the site; you can see the IP address but you cannot see what they clicked on. The whole world is moving towards https. Google is almost forcing companies to sign with a digital certificate or they will not be ranked highly. Many companies are moving towards adding a digital certificate. There is now a service online for free; you do not have to pay for a certificate any more. So increasingly companies will be signing their sites. Once they do that, communications are likely to be https.

There may come a time when many service providers will accept only secure communication. It is likely that our old protocols—http, Telnet, SMTP—will be switched off and replaced by the s version, the secure version. More and more people are using VPN connections. If you are a businessperson you will use a VPN connection if you are on the road. VPNs cannot really be cracked at all. Along with that, more people are using proxy systems where the accesses are not coming from their own computer but from another computer. Increasingly we are using public wi-fi to access the internet. It is extremely difficult to trace someone who connects to, say, Starbucks wi-fi. Very basic registration happens, usually around email addresses, and many users would not feel that they need to put full details behind that. The increasing usage of Tor is a particular problem. With Tor, you usually will not see anything at all about the IP address of the destination because each link on the chain is encrypted with a special key so there is no way you can see anything from a Tor connection.

Shabana Mahmood: So tunnelled access—such as VPNs, which many MPs use to log in when they are not on the Estate, for example, and public wi-fi—is becoming the default and therefore not easy to crack.

Professor Bill Buchanan: We have created an internet that is based on legacy protocols. They were created a time when someone had to type in the commands manually. We now have browsers, graphical interfaces and so on. These protocols can be easily breached. They can be sniffed. Anyone who listens to the traffic can crack them. So increasingly businesses and individuals are protecting themselves through the usage of tunnels. Certainly if you are a business you must ensure that your communications are encrypted over public access. If you stay in a hotel room, if you are using the public wi-fi, how do you actually know that the SSID you connect to really is the wi-fi of the hotel? It could be some intruder next door. It happened in the Far East: a whole lot of hackers in a hotel room targeted businesspeople and were continually sending vulnerabilities to them. More and more we are encrypting traffic and setting up tunnels, and it is very difficult for the UK to drive these things because they are typically driven by the cloud providers such as Microsoft, Apple and Facebook.

Shabana Mahmood: On the cloud, people with smartphones go up to the Apple cloud automatically and you get a certain amount of space. Is there any difference in security between the free cloud services and the paid-for ones such as Dropbox, as well as in how much space you get?

Professor Bill Buchanan: Obviously you pay for the security that you get. Brand reputation is very important in this space. Apple, Facebook, Microsoft and Google have their brands to protect. If there was a large-scale data breach for any of those companies, it would decimate them. Banks and the finance industry have invested a great deal in the UK in protecting data and have gone through the CBEST penetration testing. Other companies, such as retail companies and internet service providers, have not gone through the same type of testing.

Erka Koivunen: The question was about future-proofing the legislation. I was puzzled by the introduction of the term "communications service providers"—CSPs. I was not familiar with that. Internet service providers—ISPs—and the telecommunications operators; that is the normal, old-fashioned way of referring to those carrier and access network providers. I was equally puzzled to find that in the actual text of the legislation, CSPs are not mentioned. There are references to what telecommunications operators would need to do and what information would be requested from them. To me, this sounds a pretty old-fashioned way of approaching the problem of acquiring information about content or about whether an event took place in the first place. In that sense, I do not consider the Bill to be future-proof. Because there are so many references to bulk information gathering, it seems as though there is not even a proper attempt to go to non-traditional telecommunications providers to acquire the material that would be needed. Instead, the information and the traffic would be collected from the wire in bulk and then content or metadata collected with brute force, if you will. Of course, the equipment interference provisions in the Bill acknowledge that whenever you are unable to decrypt the material that you get online from the wire, you will need to go to the end point of the communication, where the material will be stored—hopefully in clear text.

I should point out that our company is actually one of the providers of those VPN type of tunnelling services. We provide a service where you can analyse yourself and encrypt your communication. You are able to move yourself virtually around the world so as to hide the

origin of your traffic. Currently, we get only a handful of "targeted" law enforcement requests for the activities of our end users. I guess I am at liberty to tell you that none of them this year came from the UK. In this sense, I am a bit puzzled as to why there is such a pronounced need to get bulk information when even the old-fashioned, more targeted means to acquire information from communications providers are not being used.

Eric King: As upsetting as I am sure it will be if every few years we have to go through a Bill of this length and size, it may be what is required. This is an area that is inherently unsuitable for future-proofing because every year technology simply provides us with possibilities that our laws do not cover squarely or clearly. Where there is a grey area, our agencies have interpreted the law to give themselves the most expansive authority time and time again. Michael Hayden, the former director of the National Security Agency in the US, summarised this by saying, "Give me the box you will allow me to operate in. I'm going to play to the very edges of that box". I am not sure I can criticise him for that. I think that the permission our agencies have is very important and it is right that they use every authority and every capability at their disposal. Nevertheless, it is important that they exercise those powers only when they have been clearly authorised to do so by Parliament.

There have been a number of circumstances over the past few years where in this country we have found that that has not been straightforwardly followed. To my surprise, in the course of litigation involving GCHQ, Charles Farr provided a statement to the court which provided an entirely novel interpretation of what constitutes an external communication. He told the court that if you and I were sending a message using our phones, that would be classed as internal, but as soon as we switched to Facebook, or any other online platform, you and I were no longer communicating. Instead, I was communicating with Facebook, and so were you, and as a result they were external communications. As a result of that, fewer protections were offered to both you and me. It seems to me that that is not right.

We had a similar experience with intelligence sharing. I will not repeat what I know you heard from Amnesty earlier on that point. More recently, I was concerned to learn that, in particular, GCHQ and our security services have taken a very expansive approach on their authorisation of what constitutes a targeted warrant. It seems that thematic warrantry has now become slightly more default than any of us were aware. I was in court a few weeks ago and heard the Treasury devil argue that the use of a general warrant—that is, that you could target on the basis of a class of persons—would be entirely permissible under the Government's current interpretation of the Intelligence Services Act, which they claim provides them with the ability to hack domestically inside the United Kingdom. These are all issues that the intelligence agencies have thought about. They have determined in secret the scope of their authority, and they are being challenged in these circumstances only because of a whistleblower who brought them to public attention. They have been brought before the courts and they are being tested. It seems to me that we will need regularly to update this law if we do not want to encourage whistleblowers to continue their practices year on year.

Q209 Lord Strasburger: Professor Buchanan, you mentioned the risk if you are in hotel of not knowing whether you are communicating with the hotel's wi-fi or something else. I have been in that position and have had my phone intercepted. It was a demonstration that was organised by F-Secure, so I declare that interest.

On the subject of future-proofing, we have heard many times during these proceedings about the very broad way that various parts of this Bill and other Bills in the past have been drafted. The explanation that we hear from the Home Office is that this is to allow future-proofing so that it can massage the definitions as time goes by. Mr King mentioned this, but neither of the others did. Is the answer to have a new Bill every Parliament, which would be every five years?

Professor Bill Buchanan: I go back to my main point that I can see cryptography and the use of tunnels increasing. There is no Bill in the world that can crack an encryption key that has been created for every connection that you make. You can legislate for it, but technically, it is not possible. The state of the art is 72 bytes. If you tunnelled on every single computer in the whole world, in a month or so, you could just crack a 72-byte key. The keys we are now using are 128 bytes or 256 bytes. It is double, double, double, double until we get to 128. It would take you a lifetime to crack 128-byte keys with current technology.

The Chairman: Is that a yes or a no, Professor Buchanan? Do you think they should be?

Professor Bill Buchanan: I can only say from a technical point of view, from a cryptography point of view, that the Bill would have to provide that cloud service providers would have to hand over the private key, have a key in escrow or have some backdoor, some proxy, on a machine. That is the only way that you would crack the cryptography problem.

Lord Strasburger: I was not talking specifically about cryptography; I was talking about all the provisions in the Bill in order to keep the provisions of the Bill current. Do we need to come back to it roughly once every five years and have a new Bill?

Professor Bill Buchanan: Certainly the way that computing is moving the pace is unstoppable.

The Chairman: Mr King, Mr Koivunen, can you say briefly, as we are beginning to run out of time, whether you agree with Lord Strasburger that we as a legislature should be renewing these provisions every so often because of the changes in technology?

Erka Koivunen: Definitely. I am a big proponent of transparency and the democratic process. Intrusive methods, such as these, should be reviewed.

Eric King: Yes, although I do not think that that should lessen the scrutiny that is put in place for this Bill.

The Chairman: On the principle of renewal, all three of you—or two of you at least are not quite sure—would be in favour.

Q210 Dr Andrew Murrison: Do these keys exist, or would they have to be created?

Professor Bill Buchanan: Do you mean the keys of the tunnels that are created or the keys that are held by the cloud providers?

Dr Andrew Murrison: The keys that are held by cloud providers.

Professor Bill Buchanan: A survey was done recently of some of the largest companies in the world. They had an average of more than 17,000 encryption keys—key pairs, as we would call them. A public key is known by everyone, the private key is what you keep secret. If someone finds the private key, they can crack the communications. The majority of companies do not know how many keys they have. Keys are being created at any given time, but companies such as Google will have a master private key which is used for its communications. That key is updated regularly. It might be six months or one year or so. That key will stay active for that amount of time. There is a revocation service on the internet that does not quite work. If the keys have been stolen by someone, what is meant to happen is that all the browsers will no longer accept that key. Unfortunately, Google Chrome does not accept revocation services by default. The keys are actually created by the cloud providers, but every session we create with our cloud services has a new key every time.

Dr Andrew Murrison: I suppose that is our safety net, is it not? We are worried about government having this information, or having access to information through keys. However, the gist of what I am asking is, are we at the moment at the mercy of providers such as Google?

Professor Bill Buchanan: Yes.

Dr Andrew Murrison: Yes, thank you. That is no comfort, is it? There are a number of these, and we presumably have no control over their internal security mechanisms, except as far as their reputation is concerned.

Professor Bill Buchanan: Only 5 per cent of SMEs have any auditing facility with their cloud provider. Only about half of large companies have some form of auditing that they can actually have on cloud services.

Dr Andrew Murrison: Thank you. Can I ask you about definitions in the draft legislation that we have seen? We have a range of descriptions, particularly in relation to communications data, such as entity and events. You might be forgiven for thinking that Sir Humphrey had drafted some of these, because to a lay person they are certainly approaching meaningless. I would be interested in your thoughts on the definitions and whether you think that they are simply creating the aforementioned box and are drafted in such elastic terms as to be maximally obliging to those in the agencies who want to pursue this data. We have mentioned, for example, the thematic warrant. It is not entirely clear to me what a thematic warrant is, and several witnesses have already said that they are concerned about the fluidity of some of the definitions used in the Bill. I would be interested in your views.

Eric King: As a broad, concerning criticism, the definitions here leave a lot of room for manoeuvre. On issues such as thematic warrantry, it is less the term "thematic warrantry" itself but the scope of the language surrounding that that worries me. The ability in particular to add and remove individuals seems very broad. The more technical terms "events" and "entities", while new to all of us, are not new to the Home Office; they are the terms that GCHQ itself has used for the past decade. GCHQ is very familiar with them and has been exploiting them to the full for a very long time. Events and entities in particular are the issues that are of most interest to our security agencies; these are the capabilities that provide them with the most amount of information. The ISC helpfully

said earlier this year that, "the primary value to GCHQ … was not in the actual content of communications, but in the information associated with those communications". I can give you a longer list, but it is very important that these definitions are tightened. A number fall in the gap. As an example, if a telephone call is intercepted and GCHQ identifies the gender of the speaker, is that an event, an entity, content? It is unclear to me.

Q211 Suella Fernandes: Clause 12, Part 2, relates to interception and refers to related communications data. I should say that new Clause 12 replaces the existing Part 1, Chapter 1 of RIPA, so it is a power that already exists. With reference to the point about related communications data, in brief it relates to communications that have been intercepted in relation to the postal service and telecommunications systems, and to assisting with the identification of a telecommunications system, an event or a location. What is your view on the clarity in that clause of the term "related communications data"?

Professor Bill Buchanan: A key aspect of this is that the IP address can never really be trusted, and any digital information that you gain typically from a home environment or electronically, again, cannot be trusted. If someone is in a home environment, they are typically on a private network and they are mapped to a single IP address, so it is very difficult to pick off the person who is actually communicating. So the ability to cross-correlate it with other information, such as location information and calls, is certainly a step forward in providing credible evidence for corroboration. This evidence on its own really should not be seen as an opportunity to look at a single source and to be able to determine the evidence from that. A great worry from our point of view is that within a private network it is very difficult to pick off individuals, so anything that can be added to that certainly helps.

Erka Koivunen: I am an engineer by background. To me, there is only the content, the payload, that we are protecting and then the metadata that describes who was communicating and where the communication was going to. There is other related information such as what type of encryption and network protocol was being used. I read with great interest about the events data, entity data and related communications data which this Bill would recognise, but to me it sounds as though you would need to tap into the network, take all the data and then start peeling the communications so that you could drop the actual payload. Afterwards, when you start dissecting the communications data for law enforcement and intelligence purposes, these terms become relevant, but when the data is acquired it does not matter how.

Eric King: In the interests of time, I will say no more than what I said previously in answer to Andrew Murrison, other than to agree with the best analysis that I have read on this point. It is by Graham Smith, who I believe you have had before you already. I know that he submitted something to the Science and Technology Committee on exactly this question. It was a masterful dissection of a complicated set of questions. I will not attempt to explain it here for fear of embarrassing myself or doing his argument an injustice, but it is one that should be rated very highly.

Q212 Lord Butler of Brockwell: I think you have partially answered this question already, but I will just ask whether you have anything to add. How clear is the definition of internet connection records in the Bill, and is it practicable to get a clear definition that will meet the purposes of resolving the IP identity?

Eric King: The first thing that needs to be remembered about internet connection records is that it is not a term that exists naturally, unlike phone billing records. It is an invented set of ideas. As a result, the first thing we should do before putting new authorities in place is wait to see the outcome of the IP resolution efforts that were made earlier this year with the Anti-terrorism, Crime and Security Act. It is still only months since that Act was passed. Its goal was to provide for IP resolution, which is the same stated goal in this Bill. It is unclear to me why we have not waited to see the fruits of that, to see where the gaps may or may not be, and to learn lessons where we can. The closest I have seen to any state attempting this elsewhere is in Denmark, which had a similar scheme over recent years but stopped it—two years ago, I believe—after it was found to be ineffective. With that, my caution would be to say that we should learn that lesson and wait for any lessons that we can learn from the IP resolution measure that was passed earlier this year.

Lord Butler of Brockwell: Going back to our earlier discussion, is not the answer that this is just a power, so the Home Office could wait for some time before it exercised it? Would you have any objection to this power being in the Bill?

Eric King: I think I would. I am not sure that the blanket retention of communications is a proportionate activity per se. In the Digital Rights Ireland case last year, the CJEU struck down a similar authority for telephone records. My position at the moment is that we should not be legislating at all in this area until cases that are going up to the CJEU are resolved, for fear of us all wasting quite a lot of our time and having to re-amend and re-adapt the law, particularly given that we could be waiting to see how the Anti-terrorism, Crime and Security Act is implemented. I think we should hold back in this area and not include it in the Bill at all.

Lord Butler of Brockwell: Do your colleagues have anything to add on ICRs?

Erka Koivunen: I would like to continue with a Danish example. I have been told by my old Danish colleagues at DK-CERT that there was an attempt to mandate that all public wi-fi providers should be required to keep session logs of where their users were communicating to. This would include not only telecommunications operators but cafés, conference halls and airports. I used to work for a telecommunications provider and we used to call these cafés hobbyists. These hobbyists would be required to gather sensitive information about who their users were communicating with and they would need to retain that information and have it available whenever law enforcement requested it. To a cybersecurity professional, that spells disaster. It is a disaster waiting to happen. Each and every store of this kind of information would be a target for computer intrusions by criminals and foreign intelligence services. One also has to remember that it would be pretty expensive for the service providers to start collecting that. In Denmark, in the end, that is why the so-called hobbyist providers were exempted from that legislation, and eventually that whole law was scrapped.

Professor Bill Buchanan: I go back to my point that proxy systems hide the IP address of the sender. Tunnelling systems hide the content. Tor systems hide the content and the IP addresses of the sender and the destination. VPNs hide the content and the source address. Many people are moving to cloud-based systems: you can run virtual desktops within the cloud. The concept of running things on hardware is going. We are moving towards almost a mainframe-type system. We have a terminal that we connect to the cloud and the

cloud exists somewhere else on the internet. Anyone who is even a little bit tech-savvy is able to pick one of those systems and hide their logs. Providers need to think through all the options and collect other information which can then be used to corroborate with the pinpoint of information that you might get from an internet service provider.

Lord Butler of Brockwell: So you would conclude that, in its present form, this is not value for money?

Professor Bill Buchanan: In its present form, from a technical point of view, it can be very difficult to find the information that is actually required from purely internet-based records. There is a whole lot of other information that we leave behind. If we have a mobile phone we can be tracked every time we make a call, and so on. There is a whole lot of other information that could be used alongside the internet record. This is not the catch-all that it could be. Ten years ago it was: you could look at anyone's record. The one company that has the whole record of every little thing we have done on the internet is Google. It has all our information. That is because it is the end point. It is the place that you go to and it will see all the information. Unfortunately, that jurisdiction is not inside the borders of this country.

Q213 The Chairman: Clauses 51 to 53 of this very long Bill talk about a request filter. What are your views on that?

Eric King: If I may, I would like to get back to the Committee on that, once I have some questions clarified by the Home Office about the exact scope of what it intends. My starting point is that it permits the same sort of data-mining at a scale that so far only our intelligence and security agencies have been undertaking, and provides that to the police, but in the name of a safeguard. Regrettably, a more detailed analysis requires more information but I will be very happy to provide the Committee with that once it is available.

The Chairman: Would you like to comment on that?

Professor Bill Buchanan: It is certainly a good way forward. Some sort of definition of the search terms that would be used would protect us from a large-scale data breach. The last thing we need is for all the information from an ISP to be leaked because a log was allowed to be taken of its site. The logs should be kept in a trusted environment and the access to them should be locked down to IP addresses and to biometrics if possible. Because they are probably among the most sensitive logs that we have, if we make sure that the requests made actually match what has been collected, we can make sure that a summary record is given to law enforcement, not the full record. Systems are easily breached. You can take data quite easily from them. It is very difficult to protect them. An abstraction around a request filter is a good way forward.

Q214 Lord Strasburger: Is it reasonable and practicable to require communications service providers to remove the electronic protections from their data when providing it to law enforcement agencies and the security and intelligence services?

Eric King: This issue has taken on increased importance due to how it seems that the Home Office wishes to apply it in future. If it intends to use it to force companies such as Apple to remove encryption or to re-architect their systems to provide a backdoor, that

would be wholly inappropriate. It would provide a lesser degree of security for us all. The Home Office needs to answer many more questions as to how it intends to use this authority. If the companies' public statements on this issue are to be believed, we should all be concerned.

Erka Koivunen: From a technical point of view, if the telecommunications operator which has been served this kind of information request is able to remove those protections, which are typically provided through encryption, of course it would make sense for these protections to be removed to enable the law enforcement and intelligence agencies to make any use of the data that they receive. However, echoing what Mr King said, there are many stakeholders in these communications service providers. Some of these providers have designed their systems specifically to employ end-to-end encryption, where the service provider is not in a position to open up the encryption. The encryption goes through the service provider's systems so that even the provider is not able to see through it. The way I am reading the Bill, it would actually ban the use of strong cryptography and strong encryption and would essentially weaken our ability to use secure online services.

Going back to the question of future-proofing, as a company that provides systems where we potentially are not able to decrypt the traffic that we pass—

Lord Strasburger: Sorry, did you say "are" or "are not"?

Erka Koivunen: We provide services that we would not be able to decrypt ourselves. We are not sure whether the Bill would concern us—whether we would be compelled to redesign our systems. I imagine that Apple will be reading the Bill with a similar sentiment. I think that it would refuse to redesign its systems in a fashion that would open up and weaken the encryption. So the Bill has some problems in the way it has been written.

Professor Bill Buchanan: Cryptography and the methods that we use in cryptography are almost perfect. Unfortunately, it is the humans who implement it who are flawed. The humans who implement security, too, are often fairly flawed in their approaches. If you ask most people whether they trust that their ISP's or CSP's security is robust enough to handle secure information such as this, I think the majority would say no, especially after the TalkTalk hack. I have many examples of where they use weak passwords and so on. If we have now got to the point where our banks can be trusted with data because of the CBEST standards and can be put to the onerous task of protecting records such as this to provide lots of different levels of access, then the ISPs and CSPs have to up their game many times over. They have typically grown from telecoms providers and have been merged from lots of little companies to provide big, heterogeneous types of organisations that are difficult to control.

The only way is with multifactor authentication. The idea that you can open up some data or a log with a single key or a single password has gone. The controls and the proving of identify is key to providing access to the data. The data should never appear offsite at all. The only way you should be able to access the data is by remote access and only through a portal. If we were to risk the opportunity of downloading a whole aggregated log on to a machine with a single encryption key then we really are opening a can of worms. CSPs and ISPs need to be thinking about access. Certainly there should be some biometrics in there—fingerprint recognition at least, along with geolocation, so that only certain

locations would be allowed access to it. A mobile phone, through out of band identity methods, is also a good way. You really must wonder, "If my password is changed by my mother's maiden name on my ISP, anyone can find out my mother's maiden name fairly simply from an internet search". If that is the level that ISPs and CSPs are now at, they need to recruit a whole lot of security engineers, architects, cloud engineers and so on. They need proper investment because this will be a massive task. The banks are soaking up all of our graduates to work in these types of environments. The next wave is that if the UK cannot produce enough cybersecurity specialists, where will we get all these new specialists? The country needs to think ahead and, I hope, invest with the ISPs or CSPs to make sure that they protect our data.

Lord Strasburger: What are the risks and benefits of allowing law enforcement and the agencies to undertake equipment interference? I mean both types of equipment interference, targeted and bulk.

Eric King: On the law enforcement side, the most powerful argument I have heard for preventing law enforcement having access to equipment interference was from the Suzy Lamplugh Trust earlier: the powers they are currently provided with are not being used to their fullest. Given the incredible intrusiveness that equipment interference could provide law enforcement, we should treat it with extraordinary scepticism. One of the issues at the front of my mind and which I have not had an answer from police or the Home Office on is how we will get around the issue that, by deploying equipment interference—what the agencies sometimes call "computer network exploitation"—we will not damage evidence that the police would later wish to seize and rely on in court. It seems that it would be incredibly counterproductive to be providing an authority in this manner that, in some circumstances, could result in criminals getting off the hook. Until I hear a compelling answer from the Home Office on that point I am not sure that we should move forward with that aspect.

In the intelligence domain it is far more severe. I struggle to understand exactly what the Government have in mind by bulk equipment interference. Every single scenario that I can conjure up seems to be within the scope of what are the not very targeted but nevertheless called targeted equipment interference powers that are there. That is because it provides them with thematic warrantry or even hacking by location. That by itself is very broad. We need to understand that, by undertaking interference, our agencies threaten British cybersecurity. They regularly hack companies in Europe and elsewhere that are not a national security threat in and of themselves. The employees of those companies are not suspected of any serious crime or criminal wrongdoing, but these companies are being attacked to allow GCHQ and other agencies to undertake further attacks. In recent years, we found out that GCHQ hacked Belgium's largest telecoms provider, Belgacom. It has also hacked Deutsche Telekom, Seagle, Stella—the list goes on and on. In doing so, they are painting targets on British companies' backs in exactly the same way and legitimising these kinds of attacks. By attacking using vulnerabilities in networks and systems that they have acquired themselves but are refusing to tell the world about so that those companies can protect themselves, they reduce the security that we collectively experience. The stockpiling of these vulnerabilities in zero-days is not considered in the Bill. Policies need to be very clearly set out about it before any consideration is made of the powers. As it stands, our recommendation to the Committee is that bulk equipment interference should be absolutely prohibited. There seems to be no good reason why such a thing could be

undertaken. Should equipment interference be permitted at all, I point the Committee to the recommendations made by Privacy International and the Open Rights Group as a result of the draft equipment code of practice introduced earlier this year in response to recommendations.

Lord Butler of Brockwell: May I ask one short supplementary on that? You say that we are putting British companies at risk by pinning a target on their backs. Foreign interceptors are not going to intercept British companies just by way of revenge, are they? They will do it anyway if they want to.

Eric King: I would hope not. Nevertheless, by using vulnerabilities and imagining that we are the only state that has discovered them we allow British companies to continue to be exposed to those threats. Instead, when British agencies find a vulnerability in networks, their presumptive position should be to disclose that to the appropriate vendor so that all companies can benefit from that security. Instead, by keeping them and using that as part of attacks, we first raise a flag, so that when those attacks are eventually discovered others will use that same attack here in the United Kingdom. Secondly, we are preventing them from being able to defend against attacks that we could be assisting them in preventing in the first instance.

The Chairman: We are getting very close on time now.

Erka Koivunen: The term "equipment interference" is pretty elegant. When I was learning information security at school we used "exploitation", "vulnerabilities" and "attacks" to describe the same things. There was no discussion of vulnerabilities or attempts to let the vendors of software products know about them. Equipment interference also refers to the deliberate introduction of those vulnerabilities and backdoors in products. In recent days, we learnt that Juniper, a big provider of core networking components that the internet is being built on, found backdoors and means to weaken encryption in its systems. This backdoor was in its code for at least two years. This was probably of use to some intelligence organisations' operations around the world. However, the UK networks, the Finnish telecommunication providers' core networks and the corporations' networks are being built by the exact same systems. They have been vulnerable to this type of exploitation for two years already and are not rushing to patch their systems. Cisco Systems had a similar case a couple of years ago that was not publicly discussed. There are many systems where it has been suspected that vendors have been compelled to introduce backdoors of this nature to deliberately weaken cybersecurity protections in favour of some intelligence organisations. I see this as a threat to civilian society's ability to conduct business online, and to e-government processes. When we cannot trust our information-processing infrastructure, we tend to avoid using it to conduct business.

The Chairman: Very briefly, Professor.

Professor Bill Buchanan: My view is that virtually everything is possible and it should be based on a risk-based approach. If something is high-risk these things should actually happen and we should be looking at exploiting vulnerabilities. As long as there is a reason for doing it and it is documented and audited, really anything is possible from a technical point of view.

The Chairman: Thank you very much indeed. Mr Warman, you have a final question before we move on to the next session?

Q215 Matt Warman: I should declare that my wife is a student at Queen Mary, but not one of yours so do not worry. If we look round the world, how does this compare to international legislation that is coming forward or is currently in force?

Professor Bill Buchanan: In France just now the access to public wi-fi is being looked at. In Kazakhstan, of all places, they are looking to implement a digital certificate where you cannot connect to a secure channel unless you use the Kazakhstan certificate. Unfortunately, the problem with that is that none of the cloud providers trust that certificate, which means that it could decimate their business and the social aspects. It has been done with the aim of improving privacy but there may also be a political agenda. It has also been shown that general certificates can be hacked. It happened when Iranian hackers got access to the DigiNotar certificate, which was a Dutch certificate, and managed to hack 300,000 users on Google and listen to their communications. Most countries are now looking at the inability to view logs. Few countries have been able to get the balance right.

Erka Koivunen: As a matter of fact, I am participating in the reform of the Finnish intelligence legislation and there are discussions about targeted equipment interference, using the terminology in this Bill. There is a pretty wide consensus that attacking foreign military installations will be something that we will see parliamentary consensus on next year, when it goes to parliament in Finland. The intelligence services in Finland have already publicly stated that they are refraining from demanding backdoors and the weakening of encryption while they seek a new mandate.

Eric King: There are lots of comparisons we could look to but we should focus on the United States as a country that we share a very similar capability with; under the Five Eyes Alliance, we also have much the same approach to issues. Over the past two years in the United States, reforms have been made to curtail NSA capability. There is one power in particular that I bring the Committee's attention to, and that is to do with bulk communications data acquisition. This is what was avowed by the Home Secretary to the Commons when introducing the Bill. While we have very little information about how this is used in the UK, in the United States this was on the front page of most newspapers. Very helpfully, two independent bodies that had access to classified material were able to look at the programme and consider it in detail. The President's Review Group on Intelligence and Communications concluded that the use of this was not essential to preventing attacks. Similarly, the Privacy and Civil Liberties Oversight Board concluded that, "we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot". This is a power that there have been two detailed reviews on in the United States and that they have decided to end. Indeed, it was just a few weeks ago that that programme was brought to a close but here the Bill is attempting to place it on a statutory footing for the very first time.

Matt Warman: That is not a technical point—if our agencies were to say that they thought it was necessary for national security, there is not a technical argument for making the observation that for political purposes or whatever they have made a different decision in a different country?

Eric King: In the country in which an operational case was made, that could be scrutinised by a series of very senior experts—who in many circumstances were very close to the intelligence community—who had access to classified material, who looked in detail at the operational case and found it lacking. My presumption is that the Committee should take the same approach until such a time in which the security services provide a public rebuttal and can show that the operational case is somehow different from the one that was so carefully scrutinised by so many people in the United States.

The Chairman: Thank you very much, all three of you, for a very interesting session, particularly Erka for coming a long way at relatively short notice. We wish you a very happy Christmas.

Witnesses: **Robin Simcox**, Henry Jackson Society, and **Professor Christopher Forsyth**, Policy Exchange

Q216 The Chairman: A very warm welcome to you both. Thank you so much for coming along this close to Christmas. We very much look forward to hearing your views on this extremely important Bill that Parliament is now considering. Apologies, too, for running a little late. I hope that it has not disturbed you. I will ask the first question, which will give you an opportunity to give the Committee your initial thoughts on the Bill. Do you think that it strikes the right balance between privacy and security? If it does not, how could it be improved? Should any other powers be included? It is really a very general question about your views on the Bill.

Robin Simcox: Many thanks for the invitation to speak here today. It does broadly strike the right balance. I might be in a minority of some of the people you have heard from so far in that I did not think that RIPA was an entirely unworkable disaster, but I appreciate that some clarity was needed with regard to bulk collection, which the Bill provides. It is also very useful for putting the powers in one place, one piece of legislation. The one thing that I might add as a word of caution is that the balance is right as the Bill is currently drafted, but I would be somewhat concerned if, during fierce negotiations in Parliament, it got watered down significantly on things such as bulk collection and the internet connection records. Those are quite fundamental powers needed by law enforcement and the intelligence agencies. The Bill is a successful piece of legislation that strikes the right balance at present, but I add that caution about losing any further powers contained in it.

Professor Christopher Forsyth: Lord Chairman, I am not an expert in surveillance, interception or security, so in a way my view on these matters is simply that of an ordinary citizen rather than an expert. I am afraid that, given the times we live in, it is inevitable that greater weight will be given to security over privacy in the balancing process than might otherwise have been the case, or even tolerable, in more placid times. To that extent, I recognise that the Bill provides for significant inroads on privacy, but it seems to me as an ordinary citizen, not an expert, that those inroads are justified.

The Chairman: Thank you both. That is very clear and concise.

Q217 Lord Hart of Chilton: We have heard in our evidence sessions a great deal about three interrelated subjects. I have three questions that I will put together. What is your view

of the proposed double lock for authorisation of certain warrants? What is your understanding of judicial review principles? What is the correct balance between the respective roles of Ministers and judicial commissioners in the authorisation of warrants? Before you answer, I put to you an answer that Shami Chakrabarti gave at an evidence session here on 9 December. She said, "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". I just wonder, since I know that you have written a paper on the question of judges taking the law unto themselves, what you think. First, is it a true double lock? Then, what do you understand the judicial review principles to mean?

Professor Christopher Forsyth: I will start with the judicial review principles, which used to be quite straightforward but are much less so now than they were. In 1984, in the GCHQ case, Lord Diplock said that there were three grounds of judicial review: procedural irregularity; illegality; and irrationality. The picture that he presents of judicial review is a situation in which you identify any one of those three grounds. If any one of those grounds is identified then the decision is open to be quashed. Outside those areas, where no ground has been established, the decision-maker—in our context, the Minister deciding whether to authorise a warrant—would be free to decide as they judged best in particular circumstances. There was a considerable degree of decision-makers' autonomy.

In his famous dictum where he set all this out, Lord Diplock also looked forward to a time in which proportionality might become part of the grounds for judicial review. So it has proved, whether it comes about through common law or through the effect of the Human Rights Act, that proportionality has assumed centre stage. This has had the disadvantage—some people would say the advantage—of making the process much more uncertain than it would otherwise have been. No one can be against proportionality in one sense—after all, we are all against taking a sledgehammer to crack a nut—but it is very easy to describe proportionality at the level of a slogan of a more abstract having the means and ends in balance. It is very easy to have that sort of description, but in reality it means a great deal of uncertainty. It is a very bold person who can predict the outcome of the decision-making process once proportionality enters the field. The principles of judicial review have become a much less certain concept than they would have been 30 years ago.

There is another consideration here that suggest that judicial review principles are, in a way, unsuitable or would have to be thought about a bit more carefully. I mentioned the three grounds of procedural irregularity, irrationality and illegality. Procedural irregularity is, of course, the principle that people should be heard and given the opportunity to make their case before a decision adverse to their interests is taken. That, of course, cannot happen in the kind of context that we are talking about—the interception of communications. It means that a whole slice of judicial review principles has been discarded for the purposes of this exercise. The effect of that would primarily be that the judges or judicial commissioners would tend to look more intensively to scrutinise more anxiously the decision-making process to make up for the fact that one is not hearing what the person adversely affected—whose communications will be intercepted—thinks about this. Is that enough food for thought?

Lord Butler of Brockwell: Can I just ask a supplementary? Would the Bill be better without Clause 19(2), about applying "the same principles as would be applied by a court on an application for judicial review"?

Professor Christopher Forsyth: That depends on what you want to achieve by the Bill.

Lord Butler of Brockwell: Would it give more effective judicial control if that clause was removed?

Professor Christopher Forsyth: I suspect that if one was to strike out that clause you would end up with more effective judicial control. In fact, there would be a real danger of judicial duplication of what the Secretary of State decides.

Lord Strasburger: Would you call that a double lock?

Professor Christopher Forsyth: One might very well call it a double lock.

Lord Hart of Chilton: So on that basis the judge would be able to supplant the Home Secretary's decision with his own?

Professor Christopher Forsyth: I suspect that would be the outcome if you were to excise the subsection on judicial review. In my view that would be a retrograde step, although it would be open to Parliament to do it if it wished to. The Secretary of State ought to be making decisions on grounds different from those of the judicial commissioner. The judicial commissioner should make up his mind and assess the legality of the process, whereas the Secretary of State must surely show that she has acted lawfully but will take many other considerations into account. For example, if you were to intercept the communications of a foreign dignitary or diplomat there might be all kinds of consequences to that decision that it is right for the Secretary of State to take into account, but it seems to me inappropriate for a judge to take into account. But if that is what you want—the same criteria being applied to both elements of that decision-making process by the judge and Secretary of State—then so be it, but what are you achieving by the double lock if they are essentially deciding the same grounds?

Q218 Suella Fernandes: I should declare an interest that I was a student of Professor Forsyth's many years ago—you probably do not remember; I was a face in a crowd. Where do you think the line should be drawn between judicial and executive decision-making power in the context of warrantry?

Professor Christopher Forsyth: As far as common or garden serious crime is concerned, it has long been the case that these decisions—to issue a search warrant, for example—are taken by a purely judicial and not an administrative process. That is absolutely right. It does not seem necessary to me to have the Secretary of State's involvement in warrantry extending to the investigation of serious or organised crime. But when one is talking about national security or economic well-being, it is appropriate that the Secretary of State should take these wider considerations into account, which are inappropriate for the judge to take into account. That is where I would draw the line. Of course, in all these areas, half-covered by secrecy or sometimes fully covered by secrecy, it is very difficult to lay down a principled position, but that would be my position. I am sorry that I do not remember you attending my lectures. I hope you benefited from them.

Suella Fernandes: I did, yes. Would you say that judges should not be involved in the issuing of warrants when it comes to national security matters?

Professor Christopher Forsyth: The Bill as it stands is a reasonable compromise in that judges can go into necessity and proportionality but they are to do so according to the principles of judicial review. If they do so according to the principles of judicial review—which means in this context that they will intervene only if they discover some ground for judicial review or a legal flaw in the decision—that seems right.

Q219 Dr Andrew Murrison: Professor Forsyth, how would you distinguish national security from serious crime? You appear to be suggesting that we should treat the two separately for the purposes of the powers discussed in the Bill. My second question is: should we not seek some sort of confluence with the rest of the Five Eyes community in the way that we determine warrantry and the various other powers in the Bill?

Professor Christopher Forsyth: Clearly, there will be cases where national security and serious crime overlap; for example, an organised money-laundering scam raising money for use in terrorist attacks or something of that kind. This is a definitional problem. Once national security became involved, I would think that it would trump ordinary serious crime and you would apply the national security criteria. But I recognise that that is a question of definition. On your question about seeking some sort of congruence with the Five Eyes community, that is so far beyond my understanding and experience—I know that the Five Eyes exist; I know very little more about them. It is clearly in the public interest that there should be close co-ordination among the Five Eyes. Whether that is achieved is above my pay grade.

Dr Andrew Murrison: I wonder if the Henry Jackson Society has a view, given its provenance.

Robin Simcox: Speaking for myself, close co-operation between the Five Eyes in this area is important but if you look at the issues to do with extraterritorial jurisdiction, what we need goes beyond the Five Eyes. If it was possible, there would be some kind of international treaty governing some of these areas because some of the things that DRIPA and the draft IP Bill look to do—for example, serving warrants against CSPs, making requests for data that are lawful in the UK but may contravene American law if those CSPs are based in the US—is where we are constantly running into the problem of overlapping jurisdictions and if there can be some progress made, as distant and unrealistic as that currently seems, considering some of the other countries that are involved in this, on an international treaty governing these things, that has to be something that we look at, to go beyond even the Five Eyes.

Q220 Matt Warman: We heard in the previous session about bulk interception being one of the most controversial issues. This always comes back to whether an operational case has been made for this sort of invasion of privacy. In your opening answers, you both indicated that you thought that it had. Can you elaborate a little more on the operational case that you see has been made?

Robin Simcox: I think it has; it has to me, certainly. One thing that the UK Government have tended to do, as opposed to the US Government, who have sometimes not been as completely savvy on this as they could have been, is provide some of the real-life case

studies of where this has been useful. The Government did this even in the draft Communications Data Bill back in 2012. David Anderson provided some examples and in the guide to the IP Bill further examples are provided. This is not just about terrorism; it is about fraud, other serious crime, stopping child exploitation, drug trafficking, et cetera. Providing those real-life examples resonates; it is too abstract without them. But I would also take it beyond that and say that the debate should be less about capacity and more about the strength of the oversight. It has been put to me in the past that, for example, we are relaxed about the Army having sophisticated weaponry because we trust the culture; we trust the oversight and that it will not be used against the population. You can apply a similar paradigm to our interception capacities. Having world-class intelligence-gathering is not a bad thing; it needs to be accompanied by extremely strong and responsible oversight.

Professor Christopher Forsyth: I agree. From my reading of the Bill and the associated documents, the case seems to be made for the necessity of bulk warrants to be granted in appropriate circumstances and the safeguards built into the Bill seem pretty considerable to me.

Q221 Lord Butler of Brockwell: Do you think that the draft Bill provides sufficient protection for legal privilege? It was put to us last week that there could be an absolute protection for legal privilege on the grounds that if a lawyer was involved in misdoing, that would remove legal privilege by itself because it would be a form of inequity. If you had a crooked lawyer, you could have legal privilege enshrined in the Bill but that would not stop the authorities intruding upon them.

Professor Christopher Forsyth: It is true that if the lawyer is found guilty of misconduct, he would not be able to rely on privilege. The difficulty is that the lawyer may be guilty of misconduct but you may not be able to prove it; you only suspect it. Again, I think the Bill has got it about right. I have no difficulty with that.

Lord Butler of Brockwell: Thank you. Did you want to add to that?

Robin Simcox: On the legal privilege side of things, I welcome the role of the judicial commissioner on this because there have been examples of the misuse of RIPA in the past, Andrew Mitchell and Plebgate being a very prominent example. But we cannot rely just on the role of the judicial commissioner here. There have to be properly trained single points of contact. Again, it goes back to the culture of the institution—the TS Eliot line about "dreaming up systems so perfect that no one needs to be good". There also needs to be a culture where powers are not wilfully and clearly misused, as seems to be the case on an isolated number of occasions with regard to RIPA and journalistic sources. So I welcome the role of the judicial commissioner but there needs to be a change in the culture as well, it seems.

Lord Butler of Brockwell: Yes, so with the role of the judicial commissioner, you think there is sufficient protection both for legal privilege and for journalists. Am I right in interpreting you both in that respect? Okay, thank you.

What about MPs? The protection there is the Secretary of State, the judicial commissioner and the Prime Minister. Is that sufficient protection for Members of Parliament, bearing in

mind that the Prime Minister may be of an opposite political persuasion from the MP in question?

Professor Christopher Forsyth: The crucial safeguard there is the judicial commissioner. I do not think that giving statutory form to the Wilson doctrine would change very much, because it is difficult to see how that statute would ever be justiciable, other than perhaps providing a clearer audit trail when one of these decisions is made. One quite understands that individual MPs of one party might not believe that the Prime Minister is much of a safeguard when he belongs to a directly opposed party, but that is what the judicial commissioner is there to do: to see that there is no skulduggery in the approval of the warrant. If the judicial commissioner refuses, it is not going to get to the Prime Minister.

Lord Butler of Brockwell: Mr Simcox?

Robin Simcox: I have nothing further to add to that.

Lord Butler of Brockwell: Would there not be some advantage in putting the Wilson doctrine in law in the sense that if it is known that in due course at the appropriate time it has to be reported to Parliament that a Member of Parliament has been intercepted, this would make the Secretary of State more wary of doing it in unnecessary cases?

Professor Christopher Forsyth: I agree. That is what I mean by there being an audit trail, but I just do not see Clause 22 actually being litigated under in the judicial review court, so it would have no legal effect.

Q222 Suella Fernandes: I have a follow-up question on the issue that Professor Forsyth raised about judges and Ministers. There has been talk in our evidence sessions about the accountability and transparency of Ministers versus judges. Lord Carlile, who was the independent reviewer of terrorism legislation, has cautioned against the involvement of judges because of the lack of transparency, electability or accountability compared with Ministers. Could you comment on the comparison between the two arms and the importance of that in this context?

Professor Christopher Forsyth: I would echo what Lord Carlile says there. I recognise that there is a very strong political drive towards having the judiciary involved in this process, but the judiciary are not accountable in the way the Executive and Ministers are. Forgive me for putting it quite as starkly as this, but one would hate to see, after there had been some sort of dreadful outrage and the death of innocents, the Home Secretary facing an angry House of Commons and saying, "Well, I authorised a warrant to intercept these communications to find out what these wrongdoers were up to, but the judge refused it", bringing judges into the maelstrom of a political dispute. That it is putting it starkly, but that is the point about accountability: that given the nature of these powers, there needs to be proper accountability, and the Executive and Ministers are accountable in a way in which judges are not.

Suella Fernandes: In what way? Could you elaborate?

Professor Christopher Forsyth: Ministers are accountable in that they will come before the House of Commons and Committees of this kind and have to justify themselves and answer difficult questions. The judges are not going to do that.

Suella Fernandes: I want to move on to another issue, overseas examples, and ask both of you whether there are any other countries that we could look to for guidance that have grappled with this issue.

Robin Simcox: This partially goes back to your previous question, too. The involvement of some democracies where the system and role of the judiciary are comparable to that of the UK—Australia, Canada, France and Germany—is significantly less than that of the UK. So there is that overseas example. The example of New Zealand, where the inspector-general of intelligence and security need not be a former judge, is sometimes cited, but I do not think you need to look to New Zealand to see how that can work well. Someone just mentioned Lord Carlile and David Anderson, neither of whom were sitting judges but both of whom were excellent lawyers who did a terrific job in the independent reviewer chair. Both have publicly done a great job in explaining that role to the public. They go on the radio and television and explain the role, and are an excellent link between the legislation and the general public's understanding of it. In this area we may decide that it needs to be a sitting judge, but the Carlile and Anderson examples provide a useful model for us here.

Dr Andrew Murrison: How do you feel that the idea of ministerial accountability in the areas we are discussing today can be lifted from the purely theoretical, since invariably when Ministers are asked about security matters in the Commons they will reply that it is not custom and practice for Ministers to comment on security matters?

Professor Christopher Forsyth: I do not think they are quite as reticent as that when they come before a Committee in private such as the intelligence services Committee. Is that not where their accountability comes through?

Dr Andrew Murrison: It is not very transparent, and I wonder whether you think that there are ways in which their decision-making can be made more transparent in real time. Of course, accountability can come to pass many years down the track, but that is of little help in the here and now.

Professor Christopher Forsyth: I think it is inherent within the intelligence services that things have to be kept secret that in an ideal world would not be kept secret, so I have difficulty in seeing how there would be accountability in real time. One can imagine that after a particular outrage and disruption and the death of civilian innocents the Home Secretary would come to the House and explain what was being done to track down the wrongdoers and to do whatever could be done to assist the victims, but would be extremely reluctant to provide any clear operational information about operations that might still be ongoing.

Lord Strasburger: But it is illegal for a Minister to discuss a warrant in public.

Professor Christopher Forsyth: I am not sure that that is the case.

Lord Butler of Brockwell: It is the case.
Dr Andrew Murrison: Do you think there may be grounds for reviewing that, given the double lock, which of course is different from practice in other countries with which we can reasonably be compared?

Professor Christopher Forsyth: Yes. I am surprised by that, quite frankly, but I think there would be occasions on which you would expect the Minister to be able to deal with the individual case, and that might allow them to discuss the warrant. So, yes, I think that should be changed.

The Chairman: Last but by no means least, Baroness Browning.

Q223 Baroness Browning: Thank you. I think Mr Simcox answered in reply to Ms Fernandes what I was going to ask, but I just wonder, Professor Forsyth, whether we could hear your views on the issue of the office of the Investigatory Powers Commissioner being led by a commissioner who has held a senior judicial position—at least as high as a High Court judge? What is your view of alternative models, such as the one used in New Zealand? I know that we have heard about other examples, but would you let us have your views?

Professor Christopher Forsyth: As I said earlier, I am cautious about the use of judges in this area. I recognise that there is a political need and a political demand for judicial involvement, but because of that general approach I see nothing wrong in principle with your inspector-general being a non-judge, as in New Zealand. If you look at some of the things that the New Zealand inspector-general has been doing, she has been acting in an entirely proper way in holding the services to account but in a way in which a judge might act. I think there are potential advantages to not having a judge, who inevitably is tied by the detail of the evidence, moving slowly and so forth. These are aspects of the judicial character. It may be good to have a non-judge dealing with these situations.

I would agree, too, that we have such good examples here of both Lord Carlile and David Anderson QC—non-judges carrying out these different legal tasks and doing so, if I may say so, with considerable success and very impressively. So I do not think that the inspector-general need necessarily be a judge, but it seems to me that very often the decision to involve the judges has been taken essentially for reasons of trust, because the other branches of government are not trusted sufficiently, whereas judges are trusted. I am not sure that that is entirely correct. When one looks at these things, as far as one can tell, not being privy to any secret information, these matters are dealt with very conscientiously and according to law entirely within the Executive at the moment.

The Chairman: Thank you both very much indeed. It has been a fascinating session. We wish you both a very happy Christmas.