INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

PRIVACY AND SECURITY INQUIRY

PUBLIC EVIDENCE SESSION 3

UNCORRECTED TRANSCRIPT OF EVIDENCE

Evidence given by:

Assistant Chief Constable Richard Berry
Gloucestershire Police

Deputy Chief Constable Jon Boutcher
Bedfordshire Police

Jim Killock
Director, Open Rights Group

Professor Charles Raab
Edinburgh University

Professor Peter Sommer
De Montford University

Wednesday 15 October 2014
(11:45 – 13:00)

Chair: I welcome our guests to this evidence session of the Intelligence and Security Committee's inquiry into privacy and security. This is the third of seven public sessions of evidence taking; we also have a number of private sessions with the intelligence agencies themselves and with Ministers. We are very grateful to you, gentlemen, for joining us this morning. For the benefit of everyone in the room, will you identify yourselves briefly?

Professor Sommer: I am Peter Sommer. I hold a number of visiting academic posts at British universities. Most of my income comes from acting as an expert witness in the sort of cases that you are interested in. I act for both prosecution and defence—obviously not in the same case. I also do a certain amount of consultancy work, which at the moment includes the Home Office.

Professor Raab: I am Charles Raab. I am professor of government at the University of Edinburgh and also the director of CRISP, which is the Centre for Research into Information, Surveillance and Privacy.

Jim Killock: I am Jim Killock, executive director of the Open Rights Group, which campaigns on civil liberties in the digital age.

Jon Boutcher: I am Jon Boutcher, deputy chief constable of Bedfordshire. I was the lead for RIPA for national policing. I am currently the national policing lead for undercover and the deputy lead for cybercrime.

Richard Berry: I am Assistant Chief Constable Richard Berry, of Gloucestershire police. I have recently taken up the national policing lead for communications data. I lead a working group developing cybercrime and digital investigation capabilities. I also chair the Communications Data Strategy Group with industry.

Q1 Chair: Thank you very much, gentlemen. We want this morning to be as informal as possible. We have a series of questions covering the issues into which the inquiry is looking, and we hope that you will feel able to assist us with your views on various matters. We would like to start briefly with a very important question about the expectations of privacy so far as a free society is concerned. We have asked others in our initial questions, what is the balance between privacy and security? Some have challenged whether there is indeed a proper question of that kind to be asked, or whether they are not alternatives but need to be combined. Mr Killock, would you like to offer us your thoughts on that to open our discussion?

Jim Killock: The first thing to remember is that privacy has become an issue for everybody in a way that perhaps it wasn't by default 40 years ago. Everybody, or a lot of people—perhaps most—have a public face that they did not have before the internet, because they may now publish and share things. Although to some that might imply that people are not bothered about privacy, it actually makes privacy more important to them, because as they decide to publish or not publish, to share or not share, or to share with some people and not others, they are having to put the question of their privacy and the extent to which they wish to either not use or exercise their privacy into each judgment that they make. Sharing your family photographs? In the past you showed everybody your photographs; now, you may put them on Facebook. Your children might be in those photographs, so do you decide to share that with the world or only with your relatives? Privacy is a much more exercised right for everybody—it is something that they are doing and thinking about constantly.

It is also worth remembering that this does apply to young people. When asked, young people say that things such as privacy and bullying are among their top concerns about the internet, not low concerns as some people might lead you to believe. It has also been found that young people choose their privacy settings much more than others.

On the broader question, it is worth remembering that privacy is a public good, something that we rely on in a society to give rights to journalists. We have had this whole question in the past few weeks about journalists' contacts being seen by the police through RIPA powers, and those journalists rightly becoming very agitated because that compromises their ability to research certain things and to speak freely in public. Our privacy has an element of public good; it is not merely a personal right to be balanced and traded off against public security.

The other element that it is critical to think about here, given the kinds of programmes we have heard about from GCHQ, is that personal security and privacy are highly aligned. If there are techniques used by GCHQ to, for instance, take over computers, take control of mobile phones or access networks, those techniques rely on things being broken in software that is generally used by companies and individuals very widely. That means that if GCHQ are using techniques that involve what are essentially not-fixed problems in software, they are deciding that their ability to sometimes investigate criminals is more important than the general security of people using software not only in Britain but globally. I am talking about the use of software bugs to access equipment. In that sense, unlike targeted surveillance of a generation ago, where you might have installed a bug in an office to listen to people, GCHQ are perhaps getting access to a computer through a bug that they know about to listen in on an office. When they use that sort of technique, they are relying on software vulnerabilities that everyone might have and that could be exploited in a different manner by either a foreign agency or criminal gangs. There is a really important point there.

Chair: Mr Killock, this is an opening comment—there will be opportunities to go into some of these other issues as we work our way through. Thank you very much.

Q2 Hazel Blears: I have a fairly general question. The ECHR provides that privacy and the right to a private family life is not an absolute right, but a qualified right, subject to constraints. I would be quite interested in your view about what the qualifications are on the right to privacy; whether there are circumstances in which an individual's right to privacy can be trumped, if you like, by the need for collective security of the nation as a whole; and where on the spectrum some of those rights might lie. I would like to ask the police to comment on that, just to set our discussion going.

Jon Boutcher: First, I agree with a lot of what Mr Killock said. Human rights is enshrined in our system, and we are very proud of it. Article 8, the right to privacy, has been adopted, but, as Ms Blears points out, that is a right that will be forgone or trumped if people behave in a manner that threatens the safety of people. There was a case not that long ago, the Kinloch case, in which, to summarise, the judge felt that when somebody comes out of their front door to peddle drugs, they forgo their right to privacy and that the police were able legitimately to watch that person conduct those activities and to record them.

The important thing to remember here—it is a very difficult question and it is not necessarily black and white—is that the game has changed. Communications data and the technology have exploded in a way that certainly I would never have forecast, and I don't think anybody in this room would have forecast. As a long-standing detective, I know that we would focus our efforts on collecting evidence against people in a fairly rudimentary and basic way. It was not technically challenging, because of the world we lived in. It is now really technically challenging. We need to balance the right to privacy and the sharing of photographs and images with the need to protect people from dangerous people—paedophiles, terrorists, murderers—who do not have the same values as, I am sure, Mr Killock, I or members of this Committee. That is a really difficult thing to do.

The important thing—there is a real link here around the right to privacy, and we respect it—is that, sometimes, there are questions that we can't answer and we need additional oversight, additional help, actually. The example might be undercover. The statutory instrument that came in in January says we need the Office of Surveillance Commissioners to pre-authorise undercover operations at 12 months. Whatever it might look like, comms data and the access to it for law enforcement agencies and the intelligence agencies has to be made available in a way that we can still protect society, but it has to be made available in a way that society is confident that we are doing that properly. Whatever measures need to be put in place to do that and whatever changes need to be made—I suspect that is more investment in oversight—we would fundamentally support. The right to privacy is no more important to any organisation or to anybody sitting here than to the police. I think that sort of captures where we are on this issue.

Q3 Fiona Mactaggart: Perhaps I should complete this triumvirate of questions and ask the professors about a point I think Jim Killock has addressed. I would be interested in your view on whether the extent of the internet has actually changed people's expectations of privacy? In terms of the way information is shared at the moment—people use supermarket cards and so on—does that change their expectations of privacy?

Professor Sommer: You could perhaps answer that in two ways. The answer is yes, there is just a lot more information available in ways that would have been extraordinarily difficult to forecast 10 years ago—maybe even five years ago. When you are talking about expectations of privacy, privacy is not just a single solid element. People might be willing to concede a certain amount of information when they go into their Tesco store and use a rewards card, or whatever it is called, because the benefit to them is that the store, in future, is more likely to have in stock the items

they actually want to buy, and every so often they might get a special offer; it does not extend any further than that. Perhaps the same might go for Amazon. The great threat of giving your information to Google in return for all of its wonderful indexing is that you receive rather more advertisements than you particularly want, but those are relatively limited. If it is a commercial entity, there is an extent to which public opinion can change things because it is fairly obvious what they are doing. There have been instances of Google, Facebook and others collecting more information than their customers felt comfortable with, organisations drawing attention to it, and Google and Facebook then withdrawing particular facilities. When you are talking about collection by the police, and particularly by the agencies, those mechanisms do not exist.

The second thing I wanted to raise is that I am not sure how far the high level goes, although I can see why people want to ask for a high level. How do we balance this and is there a magic formula for balancing? In practice, there appears to be a series of individual decisions about necessity and proportionality. If you are a law enforcement officer—I have had the opportunity to look in considerable detail at how the police handle communications data—you can see a fully audited trail for every decision that they make. It is available and, supposing that the commissioners are doing their job properly, they can see all of that. If a prosecution follows from it, the material is then disclosable under the Criminal Procedure and Investigations Act. The real problem is how will that apply to the intelligence agencies? Will there be the same sort of audit trail that can be tested? Those simple questions, which one fully understands, tend to have rather more complicated answers because the situation is more complicated than initially thought.

Professor Raab: There is a lot of conventional wisdom that people do not care about their privacy any more because of technological changes, the internet and so on. In fact, that assumption is a bit of a myth. People do care about their privacy. They also care about security, but they define it in many different ways. As has been discussed, privacy is a very complex concept with many facets, and exercised in many domains. Likewise, security is not a very clear concept, much less national security. It is difficult to find out what people expect or think about that.

There have been hundreds of surveys on people's attitudes towards privacy and so on. As part of a research project called PRISMS—not Prism, which is something else in this context—we have looked at a lot of surveys of people's attitudes to privacy, and we have done a survey ourselves of some 27,000 people across Europe. Asking people "Do you want privacy or security, and how would you balance it?" is not the way to ask the question. You have to be very crafty in asking questions about different contexts in which that may be important in order to tap what people are concerned about, what fears they have and how they regard different kinds of privacy—privacy from exposure to CCTV, privacy on the internet, privacy in terms of body searches at airports and so on. Those are different facets. If you ask the questions in a sophisticated manner, you get sophisticated answers that suggest that people do not make a trade off and do not make a balance; they look at things as they come, and they want both. There may be increasing evidence, although I cannot supply that evidence on the spot, that since the Snowden revelations more people are concerned about their privacy on the internet and when using other kinds of communications. That may be a long-winded way of saying that it is a very complex and subtle area, and to ask the question "How do you balance security and privacy?" is asking at a level that does not really get us very far.

Professor Sommer: Charles, wouldn't you agree that one of the problems with running surveys is that they depend on what precise questions you are asking and what has been in the news immediately beforehand? If there has been a terrorist outrage, it will be inclined towards security. If there have been complaints about police abuse, it will be inclined towards privacy. People do not think about it terribly coherently. Indeed, even for academics it is quite difficult to think about it coherently.

Chair: Assistant Chief Constable, I think you wanted to add something.

Richard Berry: Yes, if I may, Chair. I am really intrigued by all these debates around legal structure and oversight, and how we interpret these really complex issues. I appreciate that as the

police service, we are guests at the Committee—you scrutinise the intelligence agencies rather than the police—but perhaps I could share something that we are considering actively at the moment around the police service code of ethics. On 2 July this year, we held a masterclass of practitioners, officers and academics involved in ethics to try to work through some of these issues and how we could demonstrate almost a digital ethical accountability to the public, to go back to this notion of policing by consent.

Although we have not achieved the answer there, one of the products of that thinking and that workshop was to look at some kind of ethical governance capability to ask, explore and probe some of those difficult questions. I would make the analogy with medical research and the fact that you have ethical panels that probe and ask those really difficult questions. When the law is not quite clear, and when procedure is not quite clear, that is a kind of safety mechanism to fill the gap. That is something that we are looking at developing with the College of Policing.

Q4 Hazel Blears: We had a public session yesterday, and the idea of a code of ethics for the agencies was mentioned in a similar way. Are you sharing this work that you are doing with the agencies?

Richard Berry: Not yet, but we would be delighted to do so. We are working with academics on this, so we will very much be guided by them, but it is a space that we have not filled. In terms of public trust, transparency, accountability and being able to answer those new questions around consent in the digital age, I think it is perhaps part of the solution.

Chair: Thank you very much. I think we should now move towards the capabilities that are available to the intelligence agencies and to others. Could I ask Julian to open on this question, particularly with regard to targeted intrusion?

Q5 Dr Lewis: We will presently be coming to the much more contentious area of bulk data and the morality surrounding that, but I want to ask about targeted intrusion involving the sacrifice of an individual's privacy as a result of reasonable suspicion that they might pose direct threats to the UK. In those circumstances, do you think that it is proportionate for the intelligence agencies to investigate individuals and for those investigations to intrude on their privacy by the use of such methods as interception of communications, following them, eavesdropping on them and other intrusive methods?

Jon Boutcher: May I begin? First, there is the distinction that Richard has mentioned. We are guests here, and there is a separation between the intelligence agencies and policing. That is important, because a lot of what was talked about a short while ago—interpretation—we often rely on the courts to do. We rely on judges to interpret national security, privacy and whether we have behaved properly. I have some experience in the counter-terrorism arena as senior investigating officer for a number of investigations that often began with intelligence agencies' development of information. Without that development of information, the subsequent investigations that we conducted would never have commenced and the reality is that people's lives would have been lost. I do not think the question is whether it should happen; I think it is how it should happen—the measures to be put in place that we have with oversight through the surveillance commissioners, the interception commissioner and other bodies, and the courts. We have got to provide the reassurance for people in this room and the public that the intelligence agencies are held to account and only examine data where there is information to suggest that there is a threat, and that they are accountable for their activities. I think that is the gap that we just need to achieve the reassurance. I am sure we can design it, but it is not necessarily correct at the moment.

Professor Sommer: Surely the answer to your question has to be a very simple yes, but what you want is the audit trail. You want to have a record. It is pretty easy to do these days because most people operate on computers; computers create records. You want an audit trail that says "This is our

investigation; we think it is necessary and proportionate to get to this next stage," and if you are carrying out an ongoing interception then you need to be able to keep a record of all their actions and why you need to continue doing it.

One of the things that came out of the HMIC report on covert policing—I know we have got appropriate representations on this table—was a complaint that there was insufficient supervision of what was going on. That related to the police. It is a lot easier, as you heard down the other end of the table, to do it within the police, and the real problem is how you do it in terms of what goes on in the intelligence agencies. There, there is a direct clash of evidence. You have got assertions by representations to GCHQ, both in public and in private. "Oh, it is all very robust. There are lots of systems of authorisation." And then you have the Snowden documents, which no one has actually said are forgeries, which seem to contradict that. I do not have any easy way of resolving it, but perhaps that is something that you as a Committee can be doing. It seems to me the audit trail, which provides the justification at every stage under the necessity of proportionality test, is the way forward.

Dr Lewis: So far we have not had any witnesses saying that privacy is an unqualified right, but I did want to give Jim the opportunity to have a word.

Jim Killock: Obviously I am going to agree that, yes, targeted means of investigating people who are thought to be engaging in very dangerous activities is absolutely the right thing to do, and I would go further to say that for most civil liberties groups it is a strong preference that that is what the agencies do. That is to say: the civil liberties groups want to see criminals and terrorists investigated because they are suspected of being criminals and terrorists, rather than relying on bulk data collection and analysis, which effectively involves everybody's data being looked at and analysed. So for us, I think, there is a strong preference for this kind of approach. I think where we get into difficulties—what I was alluding to before—is questions of when investigative techniques then start relying on using vulnerabilities that are known about everybody's equipment.

Dr Lewis: You made that point. Thank you.

Professor Raab: Dr Lewis, I think you said, in the scenario you gave, that this was authorised and warranted, did you not?

Q6 Dr Lewis: Yes. What we are talking about is purely the question of whether or not intrusive measures, properly authorised, are permissible even though they infringe an individual's privacy where there is specific evidence and intelligence to suggest that the individual poses a threat.

Professor Raab: Yes, I would not disagree with that. I think it is important to apply the necessity and proportionality test. You mentioned a number of intrusive measures. It might be a question of whether you need that whole package of them, and whether each one has to be assessed in terms of its necessity and proportionality. If you can get by with two out of the three, then that is better than three out of the three.

Chair: Given the nature of the answers we will not need to spend too much more time on this particular area, but Mark and Robin, I think, you have particular points.

Q7 Mark Field: Just very briefly, really, I wondered whether, specifically, you had any concerns about looking at someone whom the intelligence agencies regard as being a threat: do you think that any of the intrusive elements we have discussed would not be justified, and where would you draw that line? I accept from what Professor Raab has said that ultimately these are often cases that are determined by the facts in the particular case, but is there any sense that you have of particular levels of intrusion that would never be acceptable or justified?

Professor Raab: Perhaps it could be that if you are not only being intrusive on the particular individual who is under suspicion, but on his family, let us say, that might raise other kinds of questions about whether that was legitimate or proportionate, because inevitably it is not simply a

single individual, but a range of domestic contacts and then, going further afield, scooping up information about others with whom that person is associated. I suppose that raises additional questions about whether it would be acceptable.

Professor Sommer: It would not be a question about technology. Overall tests are necessity and proportionality, and I do not think that you would limit yourself to any particular technology. Some technologies are obviously more intrusive than others, but the overall test stands. I do not think that you would want only to set up a rule, "Oh, whatever you do, you mustn't hack into someone's computer remotely." There may be justifications for doing that.

Chair: Thank you. Now let us move to the more difficult question of bulk collection.

Q8 Lord Lothian: It has been quite interesting that right across the board in this inquiry there has been an acceptance that the right of privacy is qualified, as it is under the ECHR, and that where reasonable suspicion is there, then directly targeted techniques are permissible. The interesting point that arises from that is that where you know someone is likely to be about to commit a crime, it is simple, you target them; but where you are looking for people who might be about to commit a crime, but you cannot prove that—I give you the suggestion, for instance, of terrorists or criminals and organised crime, who go to great lengths to conceal what they are doing, largely through use or misuse of the internet—how do you then find them if you are not allowed to collect data on a wider basis than just on a targeted basis?

Professor Raab: It is a question in part of how you define bulk collection. It is a term that we all use. I am not sure that it has a particular definition, or whether "bulk" means everything from everyone, or simply more than one or more than a very small number. One would need to judge the legitimacy of it and, indeed, the effectiveness of it, by seeing how bulk is "bulk". There may be ways. I am not a mathematician or a technologist, but I understand that there are ways of collecting more data than you need but not bulk in the sense of absolutely everything, in order then to be more precise about whom you target. I am also told that there are ways of working outwards, so that you do not specify in advance that we need to have everything, or two thirds of everything, in order to target. It may be that those are the areas that one ought to investigate with some technological expertise about how you can do these things to cause the least amount of intrusion not only on privacy but on other kinds of human values or freedoms that might be at issue in such circumstances.

Richard Berry: A couple of things come out of this. First, there is something around standardising the lexicon that we use. I made this point to Mr Anderson recently at CDSG—when we talk about "bulk", what do we mean? When we talk about "passive collection", what do we mean? What do we mean by "analysis"? There is something about the need to all talk the same language which would be really useful.

I can perhaps answer some of your inquiry from an organised crime perspective. I was in the fortunate position of co-ordinating an operation called Pentameter 2, which was a UK-wide action against human trafficking for UK sex markets. During that inquiry, we processed intelligence in bulk to discover the organised crime networks that were operating in the UK. As a result of that, we could understand all of the networks that were acting—all the networks we knew about—and how we could interdict those networks, tracing them back to Macau province in China, at the time. So there is a need for bulk analysis of collected data, and 75% of the data used in that exercise was communications data—very targeted, very bulky in terms of the exercise, but absolutely allowing us to get in front of criminal acts and to interdict those criminal networks.

Q9 Lord Lothian: Are you able to answer Professor Raab's question, what is "bulk"? In that case, how large was "bulk"?

Richard Berry: We need to define it, so I have had conversations with colleagues. We use the term "fusion"—fusion of data, bringing data entities together. I think there is a need, certainly from a police service perspective, to create some tiers of what we call "bulk", or "fusion", but that work is there to be done.

Jim Killock: The simple distinction is between "bulk" and "blanket". Where the courts have had a problem is not with "bulk" but with "blanket". What they have said is that you need reasons and specific instances, and you should look at why you need that evidence base for your investigations. But if you simply have no reason other than "it may be useful in the future", that is not permissible.

Professor Sommer: May I butt in briefly? There is a danger—police officers said it in an earlier response—of confusing the police procedure with the intelligence agency procedure. In the police procedure, when you are talking about "bulk" information, it is the communications data that is available. In practice, the communications data is held by the internet service provider, or the telephone company, and it is released under procedures set out under section 22 of RIPA. There is a clear separation and a clear audit trail.

Talking about the intelligence agencies, as we understand it they have that information and possibly intercept information, and that is all within their own control. That is then a quite separate set of problems.

Q10 Hazel Blears: That is the very issue I want to come to. There is a distinction, so I am grateful to Professor Sommer for saying that.

The agencies are sometimes described as looking for a needle in a haystack; then we have gone further and talked about the hayfield. However, the essence of the argument is that they need to have all this "bulk" collection, if you like, which they do not look at indiscriminately, so there is no indiscriminate surveillance. What they say is incredibly helpful is to have all that material, and then to be able to conduct targeted searches against that material, on the basis of patterns of behaviour or links between people, to enable them to develop targets. So these are people about whom they do not have suspicion; they do not fall within the definitions of being able to get section 8(1) warrants, and go against them in that way. But it is developing targets that could well prove to be plotting and involved in terrorist arguments or incidents.

It has been very interesting to hear people's different perspectives. Mr Killock, you said that this kind of "bulk" activity involves everyone's data being looked at and analysed. It is quite important to say that there is a difference between "bulk" collection and then what happens in terms of analysis and interrogation.

Some people take the view that collection in and of itself, irrespective of whether it is interrogated or analysed, is a breach of privacy and one that goes too far. Other people take a different view, on the basis that if it works, it is an intrusion worth accepting. However, some people take a very principled view that the privacy issues bite at the point of collection, rather than analysis or interrogation. I would be interested to hear your view.

Jim Killock: That has been the clear view of the courts; that is what happened with the DNA database, for instance. The point was that the collection of the DNA was an intrusion in and of itself. It was not the point that the courts or the police decided to go back into the database and pull out data; it was the fact that your data was in there in the first place.

So that principle has been discussed; I think it was similarly discussed with the data retention directive by the Court of Justice recently. The point is that it is an intrusion. It is not to say that it is the worst intrusion, or the only intrusion, that can take place, but it is an intrusion, and therefore it needs justification. Why are you holding this data? The court suggested that there need to be specific threats, for instance, in the case of data retention.

The question is this: when the agencies are talking about pulling out particular pieces of evidence from this field of evidence that they have gathered—the "needles in haystacks" argument—the computers that do the analytics have to look and analyse, profile and rank, everything in it. So it is not really possible to say that certain individuals are not looked at. The computers have to analyse everybody, and they profile people and decide, "That's 80% interesting, but the threshold is 90%, so we won't report it," but then perhaps the agents adjust the parameters, or maybe you start using Tor or encrypting some of your e-mails, which puts the ranking up, and then the same information is presented. The fact, I think, is that you cannot really say you are not looking at lots of data in order to produce the needles. The machines have to look at all of it, and they profile everybody for however long and for whatever reasons, in order to report back results.

Professor Sommer: There are two sorts of search that we are in danger of getting confused. One of them is when you are trying to build a general profile of what Mr Terrorist looks like, and you are going through a huge amount of data. They have particular characteristics, and everyone who meets those characteristics will therefore be of interest and we ought to inquire of them.

The danger there is what is called the false positive. It is the same sort of thing that you come across when you use Google. You type in some search terms, and it tells you it has found 50,000 references, but actually, when you look at them, only about two or three are relevant. In terms of an intelligence agency using those techniques, which are often promulgated, the danger is that if you are a false positive, suddenly you lose the opportunity for a job, you are on the no-fly list and you might get arrested, even if you are later released.

There is another sort of search, which seems to me a lot more acceptable. That is when you say, "Right, we have been investigating a group of people, and we have discovered that they have a number of contacts. We don't know very much about them, but we'd like to know what those contacts were doing in the reasonably recent past." That is classically how comms data is used by the police, who have software tools available to assist them, but there are radically different exercises, it seems to me, in how it is being used. I am banging on again about an audit trail, where people set down what they are trying to do. If it exists, it seems to me that it helps the inspector, and it gives credibility when the inspector says, "We've looked at these things, and we think the decisions are roughly right." To return to your last item of oversight, Chairman, it makes oversight more credible as well.

Q11 Mark Field: The transparency of the audit trail to which you refer may give some succour to the public that things are for the right, but is there not also a risk that too much transparency about the mechanisms and the manner in which the police and security services go about the business of trying to protect security might also lead to potential terrorists, paedophiles or others being made well aware of those sorts of mechanism? Therefore, they might go underground.

Professor Sommer: I think you can demonstrate the existence of a robust audit trail without necessarily showing people the individual entries. If people can see that over and over again, an investigator has to explain to his colleagues what he is trying to do and an investigating police officer has to get the agreement of his local single point of contact, or SPOC, and then the SPOC has to go to the senior designated officer—if all those things are properly recorded, and the access is recorded—you can demonstrate all of that without showing the individual entries. That would give you some level of comfort, and I don't see that it gives away anything very much. People know that data is collected, which is all that process tells you.

Q12 Mark Field: The broader argument about the concerns over the arguably irresponsible actions of *The Guardian* in going into great detail about the Snowden revelations was precisely that—it gave rise to public knowledge by a wider field of people about the mechanisms adopted by

security services, in so far as security is rather a big jigsaw. It would be interesting to hear from our police brethren whether they have any thoughts about what Professor Sommer and I have just said.

Jon Boutcher: There is some validity in what you say. We know that terrorists whom we capture, prosecute and convict share all the disclosure that we provide with each other. They have their own operational security debrief, so they can think, "How did we communicate? How did we operate? How did we get identified?" They are very sophisticated in doing that, which makes our job ever more difficult, so there is some validity in what you say.

Q13 Mark Field: Sorry to interrupt you, but have you noticed changes over the past 12 months, three years or five years? Is there a sense that people are getting more sophisticated about the way that they are looked at, and a sense of it becoming a much bigger problem?

Jon Boutcher: Without a doubt, and I can give you—probably not in this forum—some details around what we have seen, and how, when we were able to monitor communications, that became understood by the terrorists, who then changed that way of communicating; that was how we managed to identify the fact that they were planning an attack in the UK. That is a very valid position, and it causes me huge concerns.

We go back to comments that I made at the beginning, and Ms Blears's comments about the retention issue that Mr Killock dealt with, to do with privacy and collecting those data. The way that data are now collected, both for the agencies and ourselves, by companies, and the way that the technology has developed, means that it is not as simple as it used to be to access that phone billing. They do not collect data in that way any more. The way that they used to collect data was based simply on how they would charge us. They would collect data so that they could say, "Mr Boutcher, you owe us this much money for your phone bill this month." They do not need to do that any more. We are losing visibility and access to some of that communications information, and that is a game-changer for us.

As a result of the techniques that are available, the data collection and the metadata—enormous amounts of information—are integrated; that is because of the way these communications are collated. You have to examine and explore, as Mr Killock explained, lots of people's information, and lots of data, to extract what you need. It is a fundamental requirement that we have those data to examine; otherwise, we and the security services will not be able to keep people safe. We need to be able to demonstrate, absolutely, within the security services and intelligence agencies, that they can do that in a proportionate, justified and necessary way.

Some of the language in the media is really unfair and misleading. This is not a snooper's charter. Say that some of the mechanisms—the technology—required to do that meant that some of my phone billing got hived off, because a terrorist had contacted me in some way; I think that the public would accept that trade-off. No one is looking at those data, but there has to be a filtering of data to get the information about communications. Are there patterns of communication with areas of the world that are hostile to us at the moment? That might indicate—our threat level has now gone up, obviously, from substantial to severe—that there is a plot against us. We have to be able to do that. It might sound quite dramatic—

Chair: Could you bring this answer to a conclusion?

Jon Boutcher: It is a bit like the use of fingerprinting in investigations being taken away from us, because the world has moved on, in terms of how we operate as investigators, and how intelligence agencies work. We have to be given the tools to do the job, albeit with the right oversight. That is the key: the oversight.

Chair: Thank you. A final question in this section. Robin?

Q14 *Lord Butler:* I want to be quite clear on the witnesses' view about bulk collection, or what Mr Killock has very helpfully called blanket collection. Some of our witnesses have said that blanket

collection, under any circumstances, is unacceptable. Universally, blanket collection is subject to great filters, which narrow the information down to an infinitesimally small potential of targets that might be interesting. I think you could call that targeted investigation, because it picks out only a very small number of subjects. If it is operated in that way, is it still unacceptable?

Jim Killock: Yes. The agencies perhaps need to take the kind of approach that Charles Raab has thought about; he suggested that maybe the collection needs to be thought about, to be narrowed down. The problem for everybody is that if all of your data are collected and analysed, you start changing your behaviour. You start thinking, "Why are my data being collected? Why is the state interested in all of us? What are the potential things that are going to happen there?"

In any case, part of why this has happened is rather to do with the design of the internet and the fact that when the internet was designed and rolled out, people were not thinking about the fact that people might intercept the data along the way. The result has been that the companies themselves have started to change their behaviour, so it may not be that this is such a great technique—to simply harvest everything. That may not be quite such an available technique. It may be that in the future, the agencies have to go back to the companies. If you want Facebook's data, it has been encrypted user to user, so you have to go to Facebook. I actually think that for everybody, that is a much better way, because you can keep the accountability. You know who is going to what company and the sort of transparency that Peter Sommer suggested becomes possible. It is a much better way of behaving. It also makes everyone more secure in their everyday communications.

Richard Berry: I do caveat what Jim has just said in relation to cybercrime, because of the volume, velocity and variety of criminal behaviour on the internet and the ability to transmit lots of malware in a short space of time to targets. I can give an example of child abuse imagery. I have recently dealt with half a million IP addresses that visited that particular content, which was maliciously put into a website. Because of the power of the internet and cyber-criminality, if you do not have some form of blanket coverage across the internet, that criminality will be very difficult to intercept and deal with.

Q15 Chair: Let us move on to the question of legislation—RIPA and the other legislation under which the agencies operate. It has been suggested that RIPA is an analogue law in a digital age, and that the legislation itself is virtually incomprehensible to most people. Could I ask not just whether you think it needs to be modernised, but if you do believe that, what are the particular changes or improvements that you wish to recommend? Professor Raab, would you like to open up on this area?

Professor Raab: A little bit, Chairman. I think RIPA is generally acknowledged to be a bit of a mess, in terms of the different parts of it, the different requirements for authorisation and for warrants and so on, and therefore, it is not entirely clear. I think that has caused confusion, not only in the public, but among those who have to operate within it, about what they are supposed to do under RIPA. I think it possibly needs to be streamlined and reinforced and also made much more clear, so that the kinds of activities that go on under RIPA can be regarded as acceptable and as something that maintain or promote public trust and confidence, rather than it being seen as simply a general Act that allows all kinds of things that it ought not to. I think that is probably a short answer on that.

Professor Sommer: One of the main problems is that it is no longer easy to separate communications data and content. I generated a short note for you—I do not know whether the Clerk has distributed that. I will say orally roughly what I was saying in that.

Chair: If it is in writing, we have seen it. We are rather short of time.

Professor Sommer: Essentially, look at a typical Facebook page and ask yourself, "How do I apply the definitions?" It has obviously got content and communications data together. If you cannot separate them out easily—if it cannot be done technically, bearing in mind that the authorisation

regimes and admissibility regimes are completely different—at that point, you have to say, "We need to abandon this altogether." My view is that I would prefer to see an interception of electronic data in transit provision that would cover subscriber data, traffic data and communications data, as that appears in RIPA, which you would then see at the top-level content. I think it would be a great deal easier. It would mean that you would have to make content admissible, but I think the time is long gone when there are any sensible arguments against trying to keep it inadmissible. You would then also look at the authorisation mechanism. I think that is probably the most fundamental change in terms of the remit of your inquiry.

Q16 Dr Lewis: We have largely covered the questions of lawfulness, necessity and proportionality. Just for the sake of the record, these are the provisions that apply under the European convention on human rights and the UK Human Rights Act. The lawful purpose requirement means that interception has to safeguard national security, including relating to our economic well-being or the prevention of serious crime. Are you generally satisfied that that is a legitimate reason for the interception of communications, and that the principles of necessity and proportionality are sufficient safeguards when applying this legislation to the practical question of intercepting someone's communications?

Jim Killock: Human rights principles are exactly the right place to start. What I would really like to know from this Committee is whether the Government will recognise that when judgments are made in the next year or two about some of these practices. The one bit that you missed in your description is the question of the quality of the law. Can we, by reading RIPA, understand what is going on, roughly speaking? Do we understand the rough kinds of capabilities that the agencies are likely to have and what kind of things they might do? It is not clear from RIPA that blanket collection may be taking place under warrants. Just from that point of view, never mind any other, RIPA needs to be reviewed to make that absolutely clear. In particular there can be a public debate about whether that is acceptable.

If I may digress for a second, part of the reason why the police and others want blanket retention is because of this explosion of the sources of data. That will not get smaller; it will only get bigger. There will be more and more places where you might find data. They will not reside in a single place. The idea that we can go to the telephone company for the records is as imaginary as thinking that the BBC will provide all television in 10 years' time. It just is not happening.

Q17 Lord Lothian: Looking at RIPA and the system for granting warrants under both 8(1) and 8(4), there is a distinction at the moment between them in terms of external and domestic. There is a lower threshold for intercepting communications involving a person or entity overseas. Do you feel that distinction is valid and should continue? Secondly, under the same regime, agencies may need to cast a broader net in circumstances of looking overseas because they may not be looking at individuals. They may be looking, for instance, at groups or categories of people or even geopolitical areas. Do you think that is a significant factor in the way that RIPA should operate?

Professor Sommer: It is significant. How far you can set it down and make it a legal issue I am not sure. You need to say what sort of evidence is going to be available. One of the big problems with overseas stuff is that under the UKUSA agreement—the Five Eyes agreement—you can have an exchange of information between agencies. If there is any sort of worry such as, "Well, we are not going to provide direct intercept data. We are going to provide an interpretation, which is almost as useful", then at that point you are successfully evading any sort of form of law that exists at the moment. I am not sure what any new law would look like. It seems to me that at that level you are no longer talking about trying to give protection to the public in terms of a legal framework; you would do it in terms of an oversight framework. That might mean things like inspector generals with extensive resources rather than—I am not trying to be gratuitously rude to you—part-time parliamentarians with relatively slender resources.

Chair: We are full-time parliamentarians, you might like to bear in mind.

Professor Sommer: But you have a constituency to look after, I believe.

Q18 Lord Butler: My question relates to communications data, and Mr Boutcher has spoken about how important it is to the police. There has been some recent criticism about the way in which the police have used their powers under RIPA, particularly in getting access to journalists' telecommunications records in the case of investigation of the plebgate and Huhne cases. Some critics might say that crime was being investigated but was not serious enough to justify this degree of intrusion on privacy. A consequence of that is the suggestion that it is not enough for this authority to be exercised within the police because the police have been authorising themselves to do things that are excessive, and some people might even say amount to abuses. Could I have your comments on that and in particular whether RIPA needs to be revised in this respect?

Jon Boutcher: Those two cases have been in the press and there was a comment earlier. There has been a lot of misinformation in the press and I am a great advocate for the statutory framework of the Investigatory Powers Tribunal to investigate whether there has been any wrongdoing or inappropriate use of RIPA. What we seem to be doing at the moment is having trial by media and, of course, there are interested parties in this. I have spoken to the senior officers responsible for managing those cases —it would be wrong to talk about individual cases—and I am aware that they feel confident in the way the responsibilities were discharged. We need to let the statutory framework take its course for those matters to be investigated properly—not on various pages of newspapers—and for any findings of inappropriate behaviour or absolutely acceptable application of the legislation to come out. We have measures in place to make sure we behave properly, and they have been instigated. We just need to give them an opportunity to fulfil their responsibilities.

I was the RIPA lead for two years and the legislation was written in 2000. In many ways, it was based on society in the '80s and '90s. I spent an inordinate amount of my time speaking to barristers for legal advice, as did other interested parties. So Jim and colleagues at this table would be going for their own legal advice to understand the interpretation of that legislation with how we live our lives today. Frankly, I think a lot of that is completely unnecessary because the legislation isn't fit for the way we now live our lives and the communications challenges that we have.

That said, Parliament gave us some simple principles to apply, which we always fall back to, around necessity, proportionality and justification. We take real care in looking at article 8 and collateral intrusion. So the principles are sound, but the legislation doesn't fit the challenges we now have in society. I would encourage looking at that in future so that we don't spend unnecessary time interpreting things that the legislation was never written for.

Chair: Thank you very much. We have about 12 minutes left this morning and I want an opportunity for discussion on oversight and transparency.

Q19 Mr George Howarth: As it stands, the system is that Ministers determine and authorise the activities of the agencies. It is audited and reviewed by commissioners who have a judicial background and any complaints against that system are heard by a tribunal also made up of judicial figures. Will you comment on each of those? You referred to oversight, Professor Sommer. Do you think each stage in that process is right as it is and, if not, what should it become?

Professor Sommer: It happens quite a lot in this country that we set up institutions and then do not resource them adequately. We have an Information Commissioner with very slim resources, and the same seems to be the case with the commissioners. As a structure, if you gave them more resources and if the individual commissioners were rather more forthcoming in public, it could probably work. Notice that the individual commissioners rarely stray into the public. I do not see why they should not be able to explain rather more about what they are doing in terms of principle, because you are seeing somebody and asking them some sort of questions.

Sir Anthony May's recent report is a welcome departure from that. If you read it, it just looked too much like a sort of clubbable slap on the back, saying "These are terribly good chaps and chappesses, doing very dangerous work. There are a few slip-ups, but we have sort of rectified them." He may actually be correct in his findings, although the strong suspicion is he is not looking at enough material to form a view, because he has not got the resources, and the tone is all wrong. He is there as an auditor and you do not want the auditor of a company to go along and say, "Oh, they're wonderful people and it's a wonderful product." What you want to know is, are they keeping their books square?

To come back to this thing that I've been banging on about in most of my remarks, it is the quality of the audit trail which is available; if you have the audit trail, then they are able to carry out proper inquiries. So being able to explain what the audit trail is, plus having the commissioners or some substitute for them being more forthcoming, and better resources, that is probably the formula that you need to look at.

Q20 Mr Howarth: Perhaps Mr Killock could comment on this. There has been some criticism of the fact that the commissioner can only look at a sample, so the audit trail is incomplete in that sense. Do you think that sampling is of itself okay, but needs to be a higher level or do you reject the sampling process altogether?

Jim Killock: I think oversight and transparency comes in three or four places. Transparency starts with the quality of the law. Do we understand it? Do we understand what it is likely to produce? Then you have a question about authorisation. I do not think political authorisation is the correct way to go about it, because there are too strong vested interests and it is not clear to the public that that is going to be fair and reasonable.

Mr Howarth: So you think it should be judicial authorisation.

Jim Killock: Yes. I think it starts with judicial authorisation. Then you move through strong oversight. You then have a need for political oversight, which is the job of this Committee, but that, I feel, needs to be independent: you need to be elected by the Commons, without vetoes from the Prime Minister, and so on. It needs to be very clear to the public that you are a creature of Parliament, rather than the creature of the Prime Minister of the day.

Then, finally, we need general information about what the agencies do, in broad terms. How many people do they investigate? What size of data do they collect? What techniques do they have at their disposal? Are they able to do face recognition, location tracking, and so on? These kinds of capabilities need a public debate in order for people to agree that they are reasonable things for agencies, or whoever, to be doing. The experience of bulk collection, or blanket collection, actually occurring without a public debate says that the overall oversight mechanisms have not worked.

Q21 Chair: Professor Raab, you have given considerable thought to oversight issues. Would you care to give us the benefit of your thinking?

Professor Raab: Yes, I would. With regard to the commissioners, I think the resource question is a very serious one, as you will have heard from other witnesses. It is also a question of the relationship among the various commissioners—the whole welter of them—and how well they liaise when they have to, and how well they relate also to the Information Commissioner on certain circumstances needs to be looked at. I am not saying that they do not, but I think that needs to be looked at in particular terms.

If I may slightly divert to a broader question of the oversight of the intelligence community, there are two kinds of things in that regard. There seems to be a lack of technological understanding and capability to understand in the oversight community, as we might think about it, particularly now when there are so many issues that are not caused by but involve the use of advanced technologies,

whether it is data matching, data mining, or the analysis of bulk or blanket data and so on. I think there needs to be an increasing technological capability built into the institutions of oversight.

If you look across to the USA at the report that was commissioned by President Obama following the Snowden revelations, a report called "Liberty and Security in a Changing World", it is a very thoughtful and thorough piece of work. Among the things that they recommended was a strengthened agency called the Civil Liberties and Privacy Protection Board to oversee intelligence community activities, not only for counter-terrorism, but for foreign intelligence purposes. Another recommendation was that there should be an Office of Technology Assessment created within the Civil Liberties and Privacy Protection Board to assess the intelligence community technologies and the initiatives being used within those services, and also to support ways of using technology to protect privacy and not just to invade it.

So I think that there really is a lack. If I may say so, it is a lack that pervades parliamentary life as well. It seems to me that there is a shortage of technological capability and understanding of technologies almost from the inside. That needs to be brought into play in the oversight mechanisms, and also in the policy process by which the legislation is developed and amended in the area of intelligence and policing and so on.

Q22 Lord Butler: Do any other witnesses want to add to Mr Killock's list of the areas in which there should be more transparency?

Professor Sommer: I agree strongly with what Charles Raab has said. It is a practical problem that you need to think about. If you are looking at this sort of area, those people are probably going to need DV clearance, and the population of people who are available who have technological knowledge will need DV clearance and not be connected with the agencies that they are supposed to be criticising or overseeing. I think that that is something that you need to address. There may be ways round it. It is an urgent problem to look at.

Q23 Chair: Do any of our other witnesses have comments on transparency?

Jon Boutcher: I agree with a lot of what has been said. The only thing with transparency is that—Jim talked about some techniques—there is that trade-off. We do not want to be so transparent that we tell people who intend to hurt us how we identify them and bring them to justice. So there is a trade-off around that.

Q24 Chair: We had a particular tradition with the intelligence agencies. Until recently, they did not say anything about anything, because that was the culture of the organisations. That is changing. Mr Killock, do you think that that can be taken further without danger to the public interest?

Jim Killock: I think that it can. The thing we need to remember is that the internet and digital technologies are a public resource, so people can spot the sorts of things that agencies might be able to do. Look at what has happened since Snowden. Five years ago you might have said, "They can probably do this and they can probably do that", and you would say, "Well, technically they probably could, but I doubt that they would because they would not be so daft or do something so extreme."

Now we know, or we have got broad hints. Now people are in the opposite situation and they just assume that if it is possible, they are investigating it and doing it. It means a lot of very complicated things, but one of them is that whenever security vulnerabilities turn up, such as the Heartbleed bug, the first question on everyone's lips is, "Were the security agencies aware of this and were they doing it?" Unfortunately, that puts them in a morally dubious situation all the time. So unless it is made a lot clearer where they are really drawing the line, we are going to have a lot of people who are exceedingly suspicious and do not trust these agencies, because of the problems they start seeing in these publicly available technologies.

Q25 Chair: You raise an important point, but the point to be borne in mind is that the agencies do not themselves decide what they want to intercept or what they wish to do. They have to operate within the existing law. There may be a question as to whether the law itself needs to be reconsidered, but the agencies are not free agents in that sense.

Jim Killock: No, but I am pointing out that if a technology can be compromised in some way—if there is some gap in the technology that might make individuals vulnerable to criminals or gangs or whatever—the suspicion now is that the agencies also exploit the same problem.

Professor Raab: I would like to inject what might be an interesting historical note. You can tell from my accent that I was not born in this country, although I have lived two thirds of my life in it. When I first came here—exactly 50 years ago—the existence of the intelligence agencies was not acknowledged. "MI5? MI6? What are they? Who knows? Search me." Then we began to know the names of the organisations and then who ran them, and we began, for goodness' sake, to read their memoirs and so on. At every step of the way, it was said, "This is the end of civilisation as we know it. This is going to damage our capacity for defending national security." Transparency is a kind of incremental development, and it seems that with further steps to transparency we want to ask the question, "Is this really going to be the end of civilisation as we know it?"

Chair: That sounds a fitting way to conclude this session, which unfortunately we must now do. We are in your debt, gentlemen. Thank you for being so frank in the evidence that you have given. It has been a very important contribution to our work.

13:00
The session concluded