PRIVACY AND SECURITY INQUIRY

PUBLIC EVIDENCE SESSION 4

UNCORRECTED TRANSCRIPT OF EVIDENCE

Evidence given by:

Peter Gill
Liverpool University

Professor John Naughton
Cambridge University

Dr Julian Richards
University of Buckingham

Professor Tom Simpson
Oxford University

Wednesday 15 October 2014
(14:00 – 15:15)

Chair: Welcome to our guests who have agreed to give evidence to this session. This is one of seven public sessions of evidence we are taking, in addition to certain private sessions that we have already had. We hope that this afternoon can be a very informal exchange of views. We know we will certainly find it to be of value. We have had written submissions from most of you, which have been extremely helpful, and this is an opportunity to supplement many of those points. This session is, of course, being recorded. For benefit of others in the room, could you please identify yourselves briefly?

Professor Simpson: Tom Simpson, associate professor of philosophy and public policy at the Blavatnik School of Government in Oxford.

Dr Richards: Dr Julian Richards, co-director of the Centre for Security and Intelligence Studies at the University of Buckingham.

Professor Naughton: Professor John Naughton from the Centre for Research in the Arts, Social Sciences and Humanities at the University of Cambridge.

Peter Gill: Peter Gill, honorary senior research fellow at the University of Liverpool.

Q1 Chair: Thank you very much. As you gentlemen will be aware, the purpose of our inquiry is to look at issues of privacy and security. That covers a range of matters, such as the capabilities of our intelligence agencies, questions of the legislation that governs them, oversight, transparency and matters of that kind. We have approximately an hour and a quarter to cover quite a long and wide range of matters.

I will begin by inviting you to give a preliminary thought on your own views on the extent to which issues of privacy and security are a choice or different sides of the same coin. What is your view on how the Committee should look at these matters? Who would care to begin?

Professor Simpson: I am willing to step forward as a philosopher, I suppose. There is a view that these are, in some senses, two sides of the same coin. I am less persuaded by that. It seems very clear to me that there is a trade-off. There are certain practices which would be beneficial for security and which are adverse to citizens' privacy. The question that really confronts the Committee, and indeed the nation, is whether that is a trade-off that we should accept. It seems to me that a balancing act has to be performed here, and that is a really substantial issue.

Q2 Chair: That is interesting, because many of our civil liberties witnesses argued against that, but you take a very different view. What about your colleagues? Would they care to offer a similarly succinct opinion?

Professor Naughton: In terms of security and privacy, one of the mistakes our public discourse is making is in treating both concepts as if they were unitary and straightforward. Security, for example, is a function of two things: the level of harm we might be considering and the probability of that harm happening. A question that we have to address as a society is how we strike a balance between the risk of harm and the risk to society by overreacting. In my opinion, that judgment, currently made in private or in secret, ought to be made in more public and accountable ways.

Likewise, privacy is not a unitary concept. It is very important for liberty and is in fact, for this society, mandated by the European convention on human rights. It is culturally determined and is valuable for individuals and for society. It is also domain-dependent: we have different expectations of privacy depending on the setting we are in. I would have no expectation of privacy, for example, at Speakers' Corner, I would have less expectation of privacy on a public pavement, but I have very high expectations of privacy within my own home. Those two concepts are actually very complicated, in my opinion. The rather glib juxtaposition of the two, which says that it is one or the other and that there is a balance to be struck between them, is not quite right. It is a balance between two very complicated things.

Q3 Hazel Blears: We heard some evidence yesterday that in fact this is not a balance or a trade-off and that what there is under the ECHR is a right to privacy for family life, and that in the national security construct that right is then constrained by the authorities and the legislative framework, whether that is RIPA or something else that enables you to intrude on that privacy. I thought that concept, where it is not a trade-off, was quite an attractive proposition. In terms of the ECHR, presumably you would accept that there are circumstances in which the collective safety of the nation is put before the individual's right to privacy, subject to a legal regime?

Dr Richards: Yes, I would absolutely accept that. That is right. We have a framework in which the Human Rights Act covers those ECHR provisions. The devil is obviously in the application of proportionality and necessity—both of which are not necessarily clearly definable terms, but the basic principles are understood and are correct, in my view—and the oversight and administrative processes. So you have the regime; the key is that you operate it in appropriate ways in terms of oversight and accountability. As far as I am concerned, that is the right regime and the right way to do it.

Q4 Chair: Do we assume that there is some element of trade-off? We are living through a period of real terrorist threat that we have not always had and that we may not have in future. Is it being argued that if the threat is greater then the diminution of privacy might be something that a free society has to accept?

Dr Richards: Not necessarily. Some very fundamental changes are happening at the moment both to the nature of the threat in terms of its networked nature, which has certain implications for how we tackle it, and to the general definition of privacy in an internet age. Clearly, those things are changing. I do not think that that should mean a diminution of an expectation of privacy; it is just that the nature of how that plays out in practical terms is changing with the technology that is changing.

Q5 Sir Menzies Campbell: I will use an illustration I used yesterday, which is that a member of my family meets girlfriends by using the internet, and I occasionally go to a supermarket. We know that he will have given up a great deal of private information for the purpose of meeting someone, and when I go into the supermarket, I know that the kind of things I buy and how often I buy them will be taken to form a profile of me as a customer. How far is anything that any of you have said altered by the fact that there is a kind of voluntarism about privacy that we perhaps did not imagine certainly 20 years ago, and perhaps as recently as 10 years ago?

Professor Simpson: That goes right to the heart of this debate. We have a long-standing moral consensus that Government should not be, as standard, surveilling citizens' lives, unless there is reasonable suspicion of criminality. This is the central claim: we have a change in the understanding of privacy which justifies a change in that practice now. I think I am in very strong disagreement with that. The reason is the voluntarism with which we have disclosed details about ourselves to dating websites or to supermarkets, for example. We have done so voluntarily. The relationship in the marketplace is fundamentally different from that in relation to the state, because the state does it coercively, without anyone having a right to recourse. The moment you have clicked the end user licence agreement button, you have signed away your moral right. There is a separate question as to whether that should be regulated—whether it meets the conditions for informed consent—but that is a separate question. The fundamental point is that the bulk data collection practices that have been revealed have been happening without citizens' consent.

There is a deeper consideration here as well. One question is: what does the youth of today think should be private and what not? It may well be that they have a different understanding from an older generation. Another question is: what do we as a society want to have as an understanding of privacy in 50 or 100 years time? The crucial opportunity we have here is that in setting the legislation we send a signal to society about what we think it would be beneficial to be considered private and what to be public. Legislation has a shaping influence on society's expectations in the long term, so an expectation-setting process is happening now. In so far as we decide, collectively, that we should not be surveilling as standard citizens' private practices, we send the expectation that this indeed should be private.

To conclude, there is a really helpful historical analogy here. During the civil war, the post was routinely surveilled by the roundheads as part of the spymaster general's intelligence campaign, and there was a military justification for that at the time, but 30 years later there was a decision that letters should not be public and that they should not be something that Governments have routine access to. In some sense, it could have gone either way: the Government could have said that letters are public in the same way that postcards are public, but we would have been living with that 400 years down the line, with a form of communication through which it was not possible to open ourselves up to other people on an intimate basis. There is a similar question here about what the future is for online forms of communication—whether they are forms that we as a society want to preserve as forms that can be private and outside Government interference.

Q6 Sir Menzies Campbell: But is not your illustration precisely the point made by the Chairman? Because there was peace, it would have much easier to decide not to open people's letters. For example, in both the first and second world wars, very restrictive legislation was passed. When the wars were over—at least after the second world war—that legislation was repealed. Why? Because the circumstances were peaceful. How far does the prevailing sense of the nation dictate the extent to which privacy takes precedence over security, or vice versa? That was rather crudely put; I hope you will excuse that.

Chair: Mr Gill, would you like to offer a view?

Peter Gill: That is a good question. The big shift, I think, is that, at the end of the cold war we thought that there would be a peace dividend and so on, but what we have seen instead—it has been largely technologically driven; this is really John's area rather than mine—is that it is not that the desire of states to collect everything if they can has changed; what has changed dramatically is the potential to do it.

Despite Tom's example, my understanding of internal security for the last two or three hundred years is that the post has been regularly intercepted—always. Then it was telegrams, then radio and then telephones and so on. The state has always had the desire to do that, but it always had to be selective, because otherwise it was a completely impossible task. What has transformed the ability is the digital age, which now raises the possibility of collecting everything. As we know, both our own agencies, and the United States in particular, which is building facilities in Utah, have the specific aim of collecting and storing everything. One has a distinct sense that this is completely lacking any proportionality to the threat. We do not face the threat now that we faced in the second world war: we are not about to be invaded by a ruthless foreign state with a large army and secret police. Yes, we face a threat, but it is nothing like the threat that we faced then.

Q7 Mark Field: We can argue about the nature of the threat, but actually an internal threat might in some ways be a bigger problem. I want to go back to Professor Simpson's interesting theme about the youth of today. Given how relatively recent the internet is, the concern is that we might put in place now some sort of firm template that in the years ahead will seem very dated.

Dare I say it, the youth of today will themselves grow up. It is often said that libertarians are people who have not had children: from the moment you have children, you have a rather different view on liberty, drugs and the like. The youth of today will get older and then they may come to have similar attitudes to people now in their 40s and 50s about privacy, even though they are much more freewheeling at the moment. Is it not a concern that we look at the excitement of the internet generation without recognising that, as time goes by, there will be changes in not only the internet, but in many of the attitudes of young people to whom we think that we should be pandering, who know only that as the way of communicating?

Professor Simpson: Yes, absolutely. There are two issues. One is clearly that legislation has to be responsive to changing needs, and the needs in 20 years' time will be different from those of today. I am sure that no one disagrees with that.

The related issue is where boundaries of privacy are set—it is easier to allow something to become public than it is to recreate it as private. Once the genie is out of the bottle, we have little ability to put it back in, in that sense. In so far as we think that people who are young now might want in the future to have the benefit of a more capacious sense of what is private as against what is public, there is a responsibility not to be too quick to rush in and say, "Actually, everything is public and, therefore, we can do what we want with the data that is out there."

Q8 Lord Butler: Leaving aside voluntarism, isn't there real evidence that the public attitude to privacy has changed? I remember that 25 years ago a congestion charge was unacceptable because of

the photographing of number plates and it was unacceptable for social security records to be shared with the Inland Revenue, but now people have come to accept CCTV cameras and so on. Is there not a lot of evidence that our society's whole attitude to privacy has changed and become more relaxed?

Professor Simpson: There is that; the question then is, is that a good thing or not? The danger is that we sleepwalk into a situation where we steadily give up more and more parts of our lives and allow state intrusion, and before we know it we come to a point that none of us thought would happen, yet has become standard practice.

Q9 Chair: Is it necessarily sleepwalking, though? Maybe it is a practical, pragmatic judgment that the benefits of CCTV cameras far outweigh the intrusion of privacy. Is that necessarily to be seen as a form of sleepwalking?

Professor Simpson: It is not necessarily sleepwalking. What we have had here in the past 18 months or so with the Snowden revelations is a forcing into the public discussion of these issues. There may well be factors specific to Britain that mean that the British public is less sceptical and does not react so strongly to the kinds of data collection practice that Lord Butler identified. Partly because we have significant trust in our institutions, there has been a gentle handing over of information power to public bodies. The worry then is that without the appropriate safeguards and self-constraint of public bodies, what does that open us up to in the future?

Q10 Chair: Is there not also, though, a separate question of what degree of consent there may have been, either by the public or Parliament, to what is alleged to have been the increase in powers through the use of modern technology by agencies and by Government?

Professor Simpson: Right, yes. Surely the point of this is to register that there is significant lack of consent to that handover. That seems to me to be quite significant.

Professor Naughton: I don't think one should take passive acceptance of a fait accompli as proof of public enthusiasm. For example, in the case of CCTV in the United Kingdom, foreign visitors are always astonished by the fact that there are all these cameras and that British citizens seem to be quite relaxed about it. Part of the explanation for that might be that if you think about it from the point of view of a citizen, most of the time we are dealing with a fait accompli: suddenly cameras appear somewhere. Nobody voted for them or was consulted about them; they simply appeared. It goes on and builds, so you get a kind of disjointed incrementalism, which is one of our real problems.

One of the questions we need to ask—I hope the Committee looks at this—is, what is the direction of travel here? Where are we going to be if we go on like this? One possible answer is that we might wind up like a state such as Singapore on steroids, with an essentially passive population that is extensively surveilled, Governments that know much better than anybody else what is good for people and so on. That is one possible direction of travel for the disjointed incrementalism that we have: we have one security panic after another that leads to a perceived need for more surveillance, and so it goes. This has a destination, and one of the problems with our current discussion about it, in my opinion, is that we don't talk enough about the possible destinations.

Chair: Okay, that takes us nicely into our next section of questioning, which is on the current capabilities of our intelligence agencies. We start with the question of what is known as targeted intrusion.

Q11 Dr Lewis: We are definitely going to be coming back shortly to the key issue of bulk data, but that is not what I am going to ask about now. There has been quite a lot of consensus on the question of the propriety or otherwise of surveillance of a specific individual, but for the sake of completeness we want to run these questions past all the witnesses we are seeing. Where there is specific intelligence that gives reasonable grounds to believe that an individual poses a direct threat

to the country, do you all consider it proportionate for the agencies to investigate that individual, and for the investigation to intrude on that individual's privacy if it is necessary to find out what he or she is up to?

Professor Naughton: Yes—provided we have confidence in the integrity of the officials of the state who are doing that. In the cases from recent history, we have some questions to answer in those areas.

Q12 Dr Lewis: Does anyone dissent?

Peter Gill: I do not dissent. I agree with the general proposition, but I want to raise one issue that the Committee needs to be concerned about. In the era of big data, one of the consequences of targeting is that is has moved away from simply the targeting of identifiable individuals. In the context of the agencies not being sure precisely who or where is doing what, there is a tendency to develop profiles. We have already talked about profiles in a rather more mundane context of shopping, but here we are talking rather more significantly in a security context. What profiling is formally supposed to do is to identify groups in the population whose behaviour suggests that they may well need further surveillance. My observation here is that we need to be very careful with this, because although it sounds okay in theory, in practice, in the studies that have been done, it often comes down to forms of ethnic or racial profiling.

Q13 Dr Lewis: Yes, and you get what are called false positives.

Peter Gill: You get that as well.

Q14 Dr Lewis: I assure you that that point has been made very strongly to us and indeed in some of the papers that you yourselves have submitted. However, at the moment we are simply talking—if only to eliminate it from the rest of the discussion—about the traditional idea of it whereby there is a specific individual and we have reasonable grounds for suspecting that person may be up to no good. Is it therefore permissible to intercept that person's communications, for example, or to follow that person or eavesdrop on them? I take it that there is no dissent from that, provided that it is done with the normal lawful authorisations.

All witnesses *indicated assent.*

Q15 Mark Field: Where there is intention to intercept—whether by eavesdropping or looking at communications—are there any sorts of activities that you do not believe can be justified in circumstances where the intelligence community feels that someone poses a direct and immediate threat? We have the more traditional means—steaming letters open or tapping telephones. With the internet having such a big potential in the way that you referred to, Dr Gill, do you now think that there are areas where a hard and fast line should be drawn on this or can you see that there would be circumstances where, with all the safeguards that we are going to come on to later on—legislative and other safeguards—we can justify action?

Peter Gill: I am happy to let colleagues deal with that, as they are better on this than I am. My feeling is that I cannot believe that any Government anywhere would say, "There is a particular form of communication that we will never, under any circumstances, seek to intercept."

Dr Richards: Can I add to that? The same principles should apply as have always applied. A Government has to deliver security on those threats that it considers to be the gravest threats to the national security. In days gone by, that would have meant intercepting letters and steaming them open. The Government has to intercept whichever communications those posing the threat are undertaking. Now, that unfortunately means looking at e-mails and so on.

It would be foolish for us, as a Government, not to be having the fullest range of capabilities, specifically on the gravest of threats. There is implicit in this discussion the question of which activities we should consider appropriate for interception, and so on; I personally take the view that it should be restricted to the gravest matters of national security rather than some of the more public policy-type issues that have come into the debate more recently.

Q16 Mark Field: I am looking more from the perspective of the mechanism. As you say, the issue about a letter is that it is being sent possibly from an unidentifiable individual A to a certainly identifiable person B. The difficulty is, I guess, the collateral damage if you are harvesting a Facebook or other account of a particular individual, because then there are a hell of a lot of other people whose data is put at risk as well, and therefore their privacy is put at risk. Is that just something we have got to put up with? Or if one could start with a blank sheet of paper, could you set out a template for the way that you would like to see the state constraining the justification for what it does?

Dr Richards: Part of the difficulty here is technological, in that the mechanisms for intercepting a communication between A and B have become much more complicated than they used to be. In the good old days, you would tap a particular phone line and you knew that that was where the communication was going. The nature of global communications is such that it is much harder to do that, which means that technically you have to look in a bigger pool of communications to find the ones you are after. Part of that is a technical issue and part of that is the nature of the threat. When we are looking at things such as terrorist groups or organised crime groups, we are not usually looking at one specific individual. Any particular individual of concern is usually connected to a group of other individuals who are part of a network or part of a group. One of the things that the Government have to do in delivering security on those threats is to try to work out who the other associates are. That inevitably means that we have to look at a wider range of communications.

Professor Naughton: If I might continue on that, one of the implications of the technology and the degree of interconnectedness of individuals in an electronic world is that you obviously have to do what Dr Richards has been saying, but if you push that out to two or three levels, people on Facebook have an average of 300 friends. That means, if you are investigating them, you might have to look at 300 people, who each have 300 friends. You get to a point where a targeted investigation looks like it will investigate a significant proportion of the UK population, which is tricky. It is part of the reality of this technology.

Q17 Mark Field: I accept that. One argument would be the absolutist argument, which is that it is absolutely wrong to dig into this deep pool in this way. It sounds as though you appreciate the intrinsic concerns and dilemma that our intelligence services and police have to deal with.

Professor Naughton: Sure.

Q18 Mark Field: Have you got any solution for how we can pacify the civil liberties element, which is very concerned about that precise issue—the multiplying by 300 friends or followers at every stage of an investigation?

Professor Naughton: I think we have to recognise something that this Committee is trying to grapple with: this technology has arrived and it poses all kinds of existential challenges for us. Someone once said that technology is neither good nor bad, but it is not neutral either. It changes the world in which we have to operate. None of this is easy, and I do not think any members of this panel think that. On the other hand, my feeling is—I guess it is the feeling of some of the other witnesses—that we are not doing very well at addressing it.

Chair: Let us now move from the relatively uncontroversial question of targeted intrusion to the slightly more controversial question of what is often called bulk collection.

Q19 Lord Lothian: Listening to what has been said, there is general agreement that the right to privacy is qualified by considerations of security, where there are reasonable suspicions. There is, however, a stage before that. If you are lucky, you might find that reasonable suspicion is there, standing up in front of you, and you can act on that basis. More often than not, however, there is no sign of any activity that gives rise to reasonable suspicion, particularly in cases of terrorism arising from abroad and so on. There is therefore a preliminary stage for the security services, which have to find out whether there are reasonable suspicions in any particular area that will allow them then to invade privacy. It is that area, which has been touched on a number of times and has been referred to as bulk collection—or blanket collection, as it was described today—where I am looking for the principle. Is there an equal principle to bulk collection with direct targeted invasion in this wider area, where you have to go out and have a scattergun approach to see what you find?

Dr Richards: My feeling is that you are right that this entails a wider degree of intrusion into privacy than just going after particular targets, but, as I have said several times already today, the nature of the threat is such that we have to do that to deliver security. We are looking at networked groups of individuals; we are not looking at very specific targets. The security services, to get an appropriate handle on those groups and to find the right targets, have to do that targeted discovery process, which involves a wider degree of intrusion. We may go on to discuss that. There is a difference between how much data you collect to give yourself the pool of data in which you search subsequently and how you conduct those searches. I know a lot of the debate in this area is about whether bulk collection is the same as bulk analysis or surveillance of data, and I suspect that may be something we will get on to later, but the nature of the targets and the nature of the technology, in my view, means that we have to do those sorts of things in order to deliver security.

Q20 Lord Lothian: Is there also an element of how long you have held that data for?

Dr Richards: Yes, there is, because obviously some of that target discovery process is retrospective in a sense. You may come across a target and need to look back a few months to see who he or she was in contact with previously. Technologically at the moment, you cannot do that unless you have kept all of that data that you then go and investigate. As I have said several times, there are some real technical issues. In the future, we may be able to find solutions to that that allow us to be slightly more targeted and less intrusive, but at the moment, I cannot see any way round doing those things.

Q21 Hazel Blears: That analysis is really helpful, because we are in danger sometimes of having a polarised view, with some people saying that bulk collection is never justified in any circumstances whatsoever, because it is an intrusion on people's privacy. Even though it is not being analysed, the very act of collection is the intrusion. Other people say we could use bulk collection for all kinds of things and we should do it just because we can. There is a danger that we get polarised. The idea that technology might allow us to still create a pool of information, but a more targeted pool of information, I think is quite attractive. I do not know as yet that anybody has drawn how that might happen in practice, but I think it is quite an attractive proposition, in terms of getting to a better state there.

This question is really addressed to Professor Naughton and Professor Simpson. In your submissions, you take the view that bulk collection is useful, but that it should not be used for predictive analysis of people who might prove to be a threat—a bit like "Minority Report" and all those scenarios. You say that Government should forgo the opportunity to use bulk metadata for predictive threat investigations. You accept that this is a loss but feel it is necessary to preserve the character of a free and open society. That seems to me to be quite close to the absolutist position that

says, "Yes, you can do it, but you shouldn't do it in any circumstances." If there were evidence that bulk collection and then targeted analysis was providing targets that meant we could prevent plots and protect people's security, would you still take that view? If there were that evidence, would you still take the view that you should not do it?

Professor Simpson: Good, I was about to jump in on Dr Richards' evidence and respectfully disagree. The original question was whether there is a basic principle at play here. It seems to me that there is a basic principle, which has been a settled convention in our society, that we do not as standard have surveillance by both police and security services of UK citizens. We need a reason to depart from that convention.

Q22 Hazel Blears: Do you think surveillance is collection or analysis of information?

Professor Simpson: It is both, surely. You could have collection that goes into a vault and just disappears, and it never ever sees the light of day, but the point of doing the practice is so that it can come out and see the light of day, and this is where the false positives question come in—that there will be significant amounts of data that are looked at in relation to individuals.

Q23 Chair: Could you clarify that point? What is often indicated is that when you have material that is being collected in bulk, it is then processed through a computer that only intercepts the bit of it that corresponds to the selectors that have been programmed. The rest of it, which we are told is a very high proportion of the total, is never seen by a human eye. Against that background, does that still constitute, in your view—I do not just mean a technical breach of privacy, but is it any way a substantive breach of the privacy of the citizen, if no human eye ever sees it?

Professor Simpson: From a security perspective, there are two things you have to worry about. One is picking up people who the indicator says that there are reasons for suspicion about them, but they are not. Then, the more worrying thing is missing people who are intent on doing something, but the system fails to flag them up. So from a security perspective, that is what we are worried about. From a liberty perspective, it is the former that we are worried about. There will always be a drive from a security perspective to increase the penumbra of people whom the system indicates there is a reason to suspect when in fact there is not, and it requires a person to investigate each of those cases to decide whether further investigation is needed.

Q24 Chair: Forgive me: that is a very good analysis but I am not getting an answer to the question I asked. In your personal judgment if it is merely material that is processed through a computer—the 98% or whatever it is that does not meet any of the selectors and is never seen by human eye—does that still constitute a substantial or a significant intrusion into a person's privacy?

Professor Simpson: I think it does. I think so because of the chilling effect. The possibility of the emergence of it into the light of day then has a chilling effect backwards on the activities in question.

Q25 Chair: Is there evidence that it has that chilling effect or do you just believe it must do?

Professor Simpson: There is not quantitative evidence that we can point to but in some sense what we are looking at here is the settled judgment of our history as to what things constitute chilling effects.

Professor Naughton: First, on the chilling effect, we have evidence that people's behaviour changes when they know they are being watched. That is very old. Whether they feel the same in relation to bulk surveillance is at the moment empirically unknown. We don't know. I wanted to take on what I infer to be your view about this, which is that if it is collected by a computer, until it is looked at by a human being it is neither here nor there. Many people in the world use webmail

services like Gmail—the e-mail service provided by Google. That is free. You don't have to pay for it. What happens in fact is that Google reads your mail. It does so to decide what advertisements to display next to your e-mail. When you challenge Google about that they say, "Of course, dear boy, we don't read your mail. Our machines read your mail." I say, "Okay, that's fine. But isn't it interesting that this machine can read my e-mail and make intelligent judgments about what I might be interested in buying?" In that sense Google uses exactly the same technology as GCHQ, the NSA and other security agencies. It is the same kit.

Q26 Chair: Forgive me, but when that happens in the way you describe 99% is not being discarded. All of it is being used by Google to determine which advertisement would be most appropriate for that kind of message.

Professor Simpson: But they do that for everyone. The point I was trying to make is that the fact that we have oceans of this stuff being collected, which could not be looked at physically by any human being, does not mean, given the moderate capabilities of machine learning, of pattern recognition and so on, that you could not monitor the whole stream all the time. We suspect that in some of the security agency cases that is what they are doing. It is true that human beings are not looking at it yet but it is also the case that they have to be able to extract patterns from it because otherwise they would not know whom to target.

Q27 Dr Lewis: I want to take you back to one of Hazel's questions that we got diverted from. It was the key question to which after, it must be said, some pressure and manoeuvring, we got a straight answer out of previous witnesses. If it could be shown that the agencies' use of bulk data genuinely discovered a significant number of leads and as a result a significant number of dangerous plots were disrupted—if you could be convinced that was actually happening— would you still take the view that the benefit of being able to stop those plots was outweighed by the loss of privacy in bulk collection and that therefore bulk collection still should not happen?

Professor Simpson: If I can address that directly, I think the answer is yes. I think we are very clear on that in the submission. There is a real challenge for our national discussion here. We had the editor of *The Guardian* in Oxford some time ago. I asked him whether he would have the courage to report future terror plots which were not foiled, potentially as a result of having foregone this technology. Would he report that the victims had heroic deaths for the cause of an open society, rather than automatically assume that to be Government incompetence? That is the possibility that has to be recognised.

Q28 Dr Lewis: Thank you for that very frank answer. Before I ask everyone else whether they agree with it, could I ask you and your colleague, Professor Naughton, to expand on your alternative thesis, which is that you feel that we could perhaps have the best of both worlds, if companies preserved the data bases, rather than the Government? First, could you confirm that you generally all agree with that firm answer from Professor Simpson?

Professor Naughton: As an academic, you would expect some reservations, and I have some. The answer in principle is yes, I agree with Tom. On the other hand, the thing that is conspicuously lacking at the moment in this discussion and the thing that has impaired it is that we don't have any objective evidence that this bulk collection works, in the sense of achieving the goals that it is said to achieve.

When the review committee appointed by the United States President looked into it, they did not find it either. There were claims by the American security authorities that they had foiled six plots and so on and suddenly the number goes down and down. It may well be that this stuff is really effective at doing it, but so far I have seen no credible public evidence of that. I am perfectly

prepared to change my mind, if such evidence is ever provided, but so far it hasn't been. I think that is one of the big lacunae in this whole area at the moment.

Q29 Chair: Could your other two colleagues express their view on this question?

Dr Richards: First of all, I would respectfully not agree with Professor Simpson. If the methods we are using in bulk collection were shown to be substantively delivering security dividends for us, then I believe that those outweigh our expectations of privacy. At the same time, we should not be glib about that and say, "Away you go, fill your boots." Clearly, a very rigorous administrative process of justification, necessity and proportionality—all the things we have talked about—must be applied to that process. I believe it is being applied to that process. I would not agree that expectations of privacy would trump everything.

Peter Gill: I would say yes. My only reservation is that at the moment we do not have an institutional structure that could get the evidence that would lead on, which brings us on, perhaps, to later questions.

Q30 Chair: Let us now move on to the next question, on the legislation under which intelligence agencies operate, which is sometimes described as rather obscure and difficult to comprehend. Starting with RIPA, can I ask the panel not just do they think that RIPA needs to be modernised or reformed but, if they do, in what substantive ways is there such a requirement?

Peter Gill: The law relating to all intelligence activities in this country is relatively young. Until the Interception of Communications Act 1985, we did not have any. I think the law in all matters relating to intelligence is rather crude and is seeking to try to catch up and to do things on the hoof.

What is interesting about RIPA, as I understand it, is that it was seen by insiders as a rather good piece of legislation, because it was technology-proof. Unlike the Interception of Communications Act, which talked about telephone tapping and mail interception and metering—and that was it—RIPA was seen as covering all eventualities. Although there has been criticism that it cannot cope with the development of social media since 2000, I can see how you could read the Act and interpret it as incorporating the ability to intercept social media, which, of course, is what the authorities have been doing.

As far as the agencies are concerned, I assume that they think RIPA has been okay, so why hasn't it been okay for those of us outside? I am not a lawyer, but I have spent some time this year trying to understand RIPA, which is extremely challenging. I was much relieved when the Interception of Communications Commissioner talked to the Home Affairs Committee as a former Court of Appeal judge and said that he thought that the Act was very difficult to get your head around. That came as a great relief to me, because I am not an eminent lawyer. Even David Omand, who I think substantially wrote it—well, he did not write the thing personally, but was in a key role at the time—referred to the fact that you need a lawyer alongside you to understand it. In other words I think it is generally acknowledged, even by insiders, that the law is obscure.

So what can be done about it? As I said before, I assume that the state in this country, and any party I can imagine forming a Government in this country, in a coalition or not, is not actually going to want to say, "Okay, sorry. We should not have been doing that. We will not do that any more"—in other words, striking out bits of RIPA that give rise to bulk collection, particularly section 8(4) on certificated warrants. I cannot believe any Government would choose to do that. Therefore, my feeling is it must be made clearer. It must be better explained to the public, and Government, the agencies, Committees such as yours and academics such as us have a key role to play in explaining—if these powers are required, this is why they are required. This is a fundamental requirement in any democratic state. It was not done by RIPA. It is obscure—possibly intentionally

so. It has been exposed. It must be changed to be more certain, to be clearer. It must be explained to the public what it is all about.

Q31 Dr Lewis: I am going to ask your indulgence, Sir Malcolm. Before I ask my question about the convention on human rights and the Human Rights Act 1998, I want to give Professor Simpson a chance, because we cut him off, and I had asked him about his alternative plan about keeping big databases. With your indulgence, I would like him to have the chance to say that.

Professor Simpson: That is very kind. Just three quick reflections in response: first, clearly there is a question of degree, so if we discovered that 10,000 people a year were dying as a result of plots that could have been foiled by predictive data analysis, I am sure there would be public reconsideration of that, so the numbers are significant—but there is a burden on public disclosure of what the actual numbers are. I suppose my suspicion is that maybe they are lower than is sometimes indicated.

Secondly, I am a former Royal Marines officer, and we were for ever complaining about the quality of the kit we were given, but we got on and did the job. I would be astonished if it were not the case with the intelligence agencies that, although they would dislike certain constraints on their action, they would nevertheless get on with doing the job to the best of their ability. In that respect I have got considerable confidence in the abilities of the security agencies to protect us.

Dr Richards's point about the network nature of the threat is tremendously significant, because once you have got the tail of something you are able to branch out and follow it, so that the legal powers that correspond to targeted investigation are fit for task. The danger is actually the 9/11-style plot, which emerged relatively speaking out of nowhere. Even though that was not the case, and there were actually links, they were very tenuous links. That is the really significant danger.

Finally, it seems to us that there is at least a viable compromise—whether it is the best of all worlds is arguable—where private companies retain data, which respects the voluntary yielding of that data by private individuals, which can then be accessed by Government when there is reasonable suspicion that those individuals should be investigated further. Some investigative capability will be foregone, in that picture, but it seems to us a relatively small amount, and the significant bulk of investigatory powers are preserved.

Dr Lewis: So, for example, with communications data, the suggestion has been made that if it were kept by the telephone companies, for example, rather than by the Government, that would be less unacceptable.

Professor Simpson: Absolutely, and that was clearly the American position.

Q32 Dr Lewis: Thank you, Sir Malcolm, for allowing me to get that in.

In the European convention on human rights and the Human Rights Act 1998, the interception of the content of communications is permitted only if it is lawful, necessary and proportionate, and for a lawful purpose. That means that it has to safeguard national security, including our economic well-being, or be for the prevention of serious crime. Necessity means that the information cannot be obtained by less intrusive, alternative means, and proportionality means that it must be no more intrusive than is justified for the purpose of the investigation and must include consideration of the impact it might have on the privacy of innocent people. Do you feel that, between them, these criteria provide sufficient legitimate reasons and sufficient, effective and valid safeguards for the interception of communications?

Dr Richards: Can I dive in and say I think they do? There is a sort of logic trap here, that because some of this law is old—bearing in mind that what is new and what is old seems to have contracted over time—and because technology has changed a lot since RIPA and the Human Rights Act first came, the law must be no longer fit for purpose. I just do not think that is necessarily true. I

think it was designed in such a way, as Dr Gill described, as to future-proof it in a certain way. I honestly cannot see why what you just outlined cannot still apply.

Dr Lewis: Thank you.

Professor Naughton: May I respond? The key word in your question was "lawful". One of the interesting things we saw after the Snowden revelations and the subsequent discussions in this country could roughly be characterised thus: members of the legislature and others in authority said, "Well, whatever the Americans do, I am absolutely certain that what we do is lawful. End of story." Of course, that is a perfectly reasonable position to take; the only question you have to ask is, "Yes, but how good are those laws and how good was the law-making process?"

In relation to RIPA, for example, I was one of those who was worried about the Bill when it was going through Parliament. One of the more startling discoveries I made, and one of the most depressing discoveries I made, was that of the 635 MPs in Parliament at the time, I was guess that no more than 10 had any interest in or knowledge of this Bill. Any significant improvement made to it as it went through Parliament was made by the non-elected Members of the House of Lords.

Lord Butler: Hear, hear!

Professor Naughton: That was really staggering, I thought. This seemed to me to be a really important and potentially intrusive Act that provided an, I thought, unwarranted degree of power and discretion to the Executive, yet I and fellow campaigners could not interest many MPs in it at all. They had been told by the Home Office that this was just updating the wire tapping stuff for a digital age and so on, and they had more or less accepted that.

Just one simple example: one of the things that we predicted and warned about when RIPA was going though was that it would lead to mission creep on the part of the public authorities. In due course, we found that local authorities were using RIPA as cover, as justification, for snooping on parents who were suspected of not living in the area where their children went to school. This is a clear example—it is not rocket science, yet it wasn't spotted. I am a great believer in the rule of law, but I would like to have laws intelligently crafted by legislators who care and know about the subject, and in the case of RIPA, in my opinion, we did not have that.

Q33 Lord Lothian: I want to touch on one aspect of RIPA. We have had a lot of talk about warrants, specifically the two types of warrant—the RIPA 8(1) warrant for domestic interception and the RIPA 8(4) warrant for external communications. One of the anomalies is that the difference of threshold between the two is quite considerable. Would you like to comment on whether, if we are looking at this law, that difference of threshold and the much looser, much lower level for the RIPA 8(4) warrants, is still justifiable, or whether it should be altered?

Peter Gill: It really relates to the previous question in a sense, because the distinction between 8(1) and 8(4) is that 8(1) is the targeted one against an individual, organisation or premises—whatever—and 8(4) is the one in which a Minister also certificates a whole load of so-called selectors, which are then used to search the data collected. In that sense, 8(4) is clearly much more general and is the basis for the bulk collection we have just been talking about.

Whereas the RIPA code of practice—and of course the Act—refers to the fact that these only relate to external communications, as we discovered from Charles Farr's statement to the Investigatory Powers Tribunal which was then published, the way in which this is interpreted means that many communications that people probably assumed were internal are actually viewed as external. In other words, all their communications with Google, Facebook and so on are assumed to be external and subject to that process.

Q34 Lord Lothian: What I was really trying to ask was, given your analysis, what changes you thought should be made—if indeed you think changes should be made.

Dr Richards: Can I come back on the last point in answering that question? Even though the 8(4) warrants allow provision for a broader range of collection, they still have to apply the same principles of necessity and proportionality to the data that is collected in that way, and you still have to make the distinction between content and events data. I think it is covered legally by the overall structure of the process and, as I said before, I cannot see that there necessarily need to be any changes made to it.

Professor Simpson: It seems to me that the evidential standard should be raised for access to metadata or communications data. There is the notion of directed surveillance—that category within RIPA—and if you think about what kinds of data are included in metadata, it seems to me to meet the significance for the person being surveilled that normally requires directed surveillance authorisation. In particular, you get GPS data under metadata, and the level of detail of your life that is revealed by that is equivalent to having someone tail you around town for the day. In order to tail someone, you require authorisation at the level of directed surveillance. So it seems to me that access to metadata should require the same level of authorisation.

Q35 Hazel Blears: Just for clarification, that is similar to evidence that we have heard from lots of people—they feel that the area in which RIPA is out of date is the distinction between data and content, as that is now blurred because of the rich picture that you can get from data, and the distinction between internal communications and external communications is blurred now because if one end of the communications is abroad there is a different regime, and so many of the servers and routers are abroad anyway. Those two areas have been put to us as areas where the current distinctions are artificial and outdated. Is that broadly your view?

All witnesses *indicated assent.*

Q36 Fiona Mactaggart: Talking about things that go overseas, one of the issues that we have had evidence about concerns the extent to which agencies might share collected information with agencies in overseas countries. Obviously, because of the international threat of terrorism, such sharing is inevitable. But what should we recommend that that should be subject to?

Peter Gill: This international sharing is a very important question. We are in a treaty with the United States, Australia and New Zealand dating back about 60 years. Its whole logic is information sharing based on signals intelligence—that is the sort of stuff we are talking about. So this has been happening for donkey's years. Since 9/11 it has been happening a great deal more. While there will be operational rules under which agencies share, the literature is clear that much of this sharing is entirely informal. It is not necessarily subject to formal agreements. In other words, most of this sharing remains beyond any existing form of oversight at all. As we discovered with the rendition controversy—this Committee tried to look at it, other countries tried to look at it and the Council of Europe tried to look at it—everyone is blocked, because no national agency will share with you information it has received from a foreign agency. There is currently no mechanism for the oversight of intelligence sharing.

In RIPA, there is one reference to information that our agencies may pass abroad, but on what we may receive there is no restriction at all, bar one, and that is the restriction on information which is believed to have been obtained by torture. Otherwise, there are no restrictions at all. There is no law and there is no oversight of this whole area, so it is, for you, a considerable challenge. I would say it can only be done by a Committee such as yours, working with colleagues abroad—the biennial review conference that I know you attend—and making more of those links to try to get a grasp on this whole area.

Q37 Lord Butler: Supplementary to that, is it not the case that with any information, any intelligence, that our agencies get from overseas partners, our agencies are still constrained by the

operation of our law? It has to be necessary, legal and proportionate and, if they are going for content, they have to have a warrant. Does not that help to satisfy you?

Peter Gill: No, it doesn't. There is a subtle distinction here. I think the law here would be clear. If our agency is receiving from a foreign agency some kind of raw data, then I can see how our own legal restrictions might well apply. Intelligence agencies do not really like sharing raw data with each other because it tends to betray sources and methods, but they will share a report, a summary, a synopsis, or something like that. That is developed intelligence, not raw data, and I do not think there is any legal restriction in RIPA or anywhere else on their receipt of that.

Q38 Lord Butler: Not on the receipt, but on the use of it. Unless it is within the powers of our agencies, they cannot use a report of that sort. That is my understanding. Is that right?

Peter Gill: But it could inform their future intelligence and information-gathering activities though, couldn't it?

Q39 Lord Butler: While you have the floor, Mr Gill, I wanted to pick up on something you said earlier. When we were talking about the public's acceptance of the activities of the authorities, you said that a lot is acceptable "provided they have confidence," and then at the end you added, "which has been weakened by recent events." Could you elaborate? What did you have in mind?

Peter Gill: I think it is the whole area we are talking about. The entire British public have not consumed the Snowden material, of course, because it has only really been published in one or two bits of the press, but if you look at the poll data, such as it is, from the past 15 months—I realise that one has to take poll data with a pinch of salt—it is clear that there is public concern about this form of intelligence gathering. My other comment was based on the fact that this is not the only bit of intelligence the Intelligence and Security Committee cover. If we look at other issues—I am thinking particularly of the undercover policing controversies—we see in the past two or three years a series of controversies around the use of intelligence by the state, be it the police or intelligence agencies, that make people sense that something is not right.

Professor Naughton: May I follow on from that? I think a fundamental difficulty is that, because of the sensitivity of these matters, because of the way the security authorities work, because of the way this Committee works and so on, essentially the position often is that the public are being told, for example, "The threat's very serious," and if you ask, "How serious?" the response is, "We couldn't possibly tell you. We know, but you don't." What it comes down to in the end is essentially a proposition, "Trust us," and in the past two or three years we have seen a number of startling examples of where serious British public institutions have demonstrated vividly that they are not worthy of trust. We are talking about the Metropolitan police, we are talking about Parliament itself in relation to expenses, and so on and so on. In those circumstances, it is hardly surprising that there is a certain level of public scepticism about chaps in suits and ties telling you, "Don't worry, it's alright—it's terrible, but we have it."

Q40 Chair: What you say is of course correct, but it has to be balanced by the fact that no one has yet produced a formula that enables the Government to share this information with the British public without it becoming available to the bad guys in other parts of the world who are trying to do us harm. In a sense, I think the debate is not about, "Trust us," but is about Government asking to be trusted only in areas where it genuinely cannot reveal information without doing damage to the very objectives that it is trying to protect.

Professor Naughton: I agree, but trust has to be earned.

Chair: Sure, but that means that you make the request to be trusted only when it is absolutely necessary. There have been occasions over the years when either Governments or the intelligence agencies themselves have been more nervous about transparency than they needed to be. The very fact that the agencies have become much more transparent in recent years without any obvious harm to their interests demonstrates that perhaps they were over-cautious in the past.

In the last few minutes that we have, I invite you to offer any views you have to the Committee about the questions of oversight and transparency, and if you believe there are important arguments for change.

Peter Gill: On oversight, my feeling is that what has been exposed in the last two or three years is the rather haphazard and compartmentalised nature of the structures we have. The ISC is at the centre of this, and in a parliamentary democracy that is absolutely right. The other parts of the structure—the commissioners and the tribunal—have developed in a piecemeal, haphazard way since 1985 and it is now clear that collectively they do not provide an adequate oversight structure.

I would ask the Committee to give serious thought to suggesting the establishment of an independent body that would combine the three commissioners' offices. The mandate for that office would be the oversight of covert investigation in this country. We are not just talking about communications interception: we are talking about undercover policing and various other forms of information gathering, as you well know. It is not appropriate that interception communications is done in one place, undercover policing is done in another, and undercover work by the intelligence agencies is done in yet another place. It is a mess. I would strongly suggest a single body which could also receive complaints and present cases to the tribunal, rather than the tribunal doing it all themselves, which is not appropriate—it is not subject to due process. It would receive complaints or concerns from employees—we have had a staff counsellor for almost 30 years now but that is very secretive and no one really knows how it works. We need joined-up oversight, not the fractured system that we have at the moment.

Professor Naughton: For me and my colleagues in academia, we would want to see oversight that is technically informed and competent in this area. We have oversight by lawyers, judges and parliamentarians, most of whom are not up to speed on this technology. One of the important requirements for credible oversight would be the inclusion in oversight processes of technical experts who are independent and have security clearance.

Dr Richards: The ISC has the potential to be an entirely appropriate and effective form of oversight. There is a case for perhaps some changes to it. The move from being an appointed Committee of parliamentarians to being a proper parliamentary Committee is the right move. I quite like the idea of bringing in some technical experts to the process, and there is a lot of merit in that. The basic principle goes back to an example that we had a short while ago of international relationships between intelligence agencies. I hope that ISC could scrutinise those relationships and look at what is going on, at what data is being shared with overseas partners and is that appropriate. If those provisions are in place and the ISC has sufficient powers, that is an acceptable level of oversight for me.

Chair: On the recommendation that ISC has more access to technical information, we can and have used technical advisers when we have thought it to be appropriate in particular inquiries, but there may be a case for expanding on that in the way that you suggest.

On behalf of the Committee, I thank the panel for your very helpful contributions. We have had the benefit of both your written submissions and your oral evidence, and they have given real added value to our deliberations. Thank you very much.

15:15

The session concluded