INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

PRIVACY AND SECURITY INQUIRY

PUBLIC EVIDENCE SESSION 1

UNCORRECTED TRANSCRIPT OF EVIDENCE

Evidence given by:

The Rt. Hon. David Blunkett
Member of Parliament

Charlie Edwards
Director of National Security, RUSI

Professor Anthony Glees
University of Buckingham

Baroness Onora O'Neill and Rebecca Hilsenrath
Equality and Human Rights Commission,

Tuesday 14 October 2014
(10:00 – 11:45)

Chair: It is my pleasure to welcome you all to this evidence session for our inquiry into the appropriate balance between the individual's right to privacy and our collective right to security. Can I mention first of all that this is a recorded session and there will be a transcript of the evidence? We are very grateful to the witnesses this morning for their attendance. Perhaps I could just invite each of you, in half a sentence, to indicate who you are and your background, for the purpose of the transcript? David Blunkett, would you like to start?

Mr Blunkett: I am David Blunkett. I am Member of Parliament for Sheffield, Brightside and Hillsborough. I am relevant to this discussion as the former Home Secretary.

Charlie Edwards: I am Charlie Edwards, Director of National Security and Resilience Studies at RUSI.

Professor Glees: I am Professor Anthony Glees, Director of the Centre for Security and Intelligence Studies and Professor of Politics at the University of Buckingham. I was previously a Professor of Politics at Brunel University.

Baroness O'Neill: I am Onora O'Neill. I chair the Equality and Human Rights Commission and am a Cross-Bench peer. I am a philosopher in private life.

Rebecca Hilsenrath: I am Rebecca Hilsenrath. I am the chief legal officer at the Equality and Human Rights Commission.

Q1 Chair: Thank you for those comments. I welcome you and say that we are very grateful to you both for your written submissions and for your willingness to give oral evidence. Today's session will cover a number of themes on expectations of privacy; on targeted intrusion, but also on what is often referred to as bulk interception; on legislation; and on oversight issues.

I should point out generally that our inquiry began in February this year, since when we have received a wide range of written evidence from Government, from the agencies and from private advocates, the media, and other members of the public. We have taken oral evidence already from the intelligence agencies. We are due to take evidence also from the Foreign Secretary and the Home Secretary. Over the course of these public evidence sessions, we will be taking evidence and hearing the views of people with a wide range of views, some of which have already been brought into the public domain.

I should make the point, of course, that this is a public session. It is not the first public session of this Committee, but they are relatively rare events. Because they are public sessions, we cannot deal with classified material, either in the questions we ask or in the answers we expect and hope for from our witnesses.

With these opening comments, can I now move to the first general question that we would like to have your thoughts on? This is the question of expectations of privacy. What should be understood by the right to privacy? Is it something which is an absolute right, or is it something which is qualified in relation to the issues that this inquiry is looking at? David Blunkett, would you like to open the response?

Mr Blunkett: First, thank you very much for inviting me. Secondly, I did put a substantive submission in much earlier in the year. It has not necessarily been overtaken—obviously time has passed—but I am very happy for that to go online, if that would be helpful in the debate.

I think we have always taken the view in this country—it is part of our Anglo-Saxon and philosophical view—that we have to deliberate and be able to demonstrate that there is an absolute overriding imperative before we intrude into people's privacy. The emergence of online and cyber has changed dramatically the nature of the debate in two ways.

First, it has technically made it possible to intrude, to intercept, to be able to examine people's private data in a way that was not as obvious in the past. I make the point in my report that envelopes were unsteamed and old-fashioned telecommunications used to have the local village gossip listening into people's telephone calls from the switchboard. But the world has changed. The second part of that—it is a paradox—is that very many young people are prepared to give up their privacy quite readily in order to be able to demonstrate what they are doing in life and to communicate with their friends.

So we do have a paradox, where we desperately need ways of ensuring that we reassure the public as a whole that we are not, as a state, intruding on privacy. We need to be able to protect people from intrusion on privacy in terms of the data that they give up to private enterprise, and we need to persuade people that they need to understand and have greater information and education on what they are doing in daily life, which actually then demonstrates an erosion of their own privacy. These things are contradictory.

Q2 Hazel Blears: I want to direct my question at Baroness O'Neill and her legal adviser. It is about the ECHR. As we all know, the ECHR does not guarantee privacy above everything else. Privacy is a qualified right, rather than an absolute right, where there is a balance to be struck, and that really goes to the heart of our inquiry, which is about where that appropriate balance is. What is

your understanding of the qualifications on the right to privacy, and is it acceptable for the needs of society as a whole to be put before an individual's right to privacy? Could you start us off on what, as I said, is at the heart of our inquiry, which is where that balance might lie from an ECHR point of view?

Baroness O'Neill: In the European convention, privacy, of course, is a qualified right; article 8 states that it is a right to privacy in the home, the family and the correspondence. Then, in part 2 of article 8, some of the qualifications are listed, and of course they include "national security". Let us also note that they include "health and morals", so there are quite a lot of qualifications.

The question then arises: what would be a reasonable and effective way of securing that? The metaphor of balance is often used; I do not think it is particularly revealing. However, it is clear that there has to be an institutional structure, as we have—or by intention have—in RIPA, whereby there is constraint on the pursuit of people's private information, but the breach of the constraint has to be justified by showing that what is done is necessary and proportionate. Again, those are very abstract phrases, but I think their interpretation has to be contextual and I hope that the Committee can clarify the sorts of regime, or perhaps one regime, that could secure necessary and proportionate intrusions only.

Hazel Blears: We will come later to legislation, oversight and transparency, which will amplify those issues.

Q3 Sir Menzies Campbell: A member of my family meets girlfriends by utilising the internet. In order to do so, he reveals quite extraordinary details about his own life: where he lives; his circumstances; things of that kind. We also know that if we go into one of the supermarket companies and buy certain articles, then they build up a profile of us. How far do you think that that acceptance by members of the public intrudes upon this balance that you describe? If people are willing to make that kind of information about themselves available, does that have any impact on determining where the balance should be struck?

Professor Glees, perhaps you would like to deal with that.

Professor Glees: First, thank you for asking me to come and speak to you.

What I would say is what I have said in my written submission to you: I do not believe there is an absolute right to privacy, but I do believe there is an absolute right to lawful security in the pursuit of our freedom. So, no absolute right to privacy and, as Lady O'Neill says, privacy is only a qualified right in the European convention.

The way I see it is that you can have security without liberty but you cannot have liberty without security, and that is an overriding principle of being in a free, liberal democracy. In my view, the right to privacy is weaker now because of the way that people behave, and willingly behave, because of the needs of medical science to pull data, in order to deal with life-threatening diseases, and, of course, in order to deal with the terrorist threat that we face.

I am very clear that we need a security community that is effective, and we need to give it the tools that it needs to be effective. That means invading people's privacy on occasions, but it must be done lawfully. However, when I wrote to you originally, there was no talk of the UK leaving the ECHR, and I think that presents us with a very new and very serious situation. I believe we have one of the best intelligence communities in the world, but I would be mortified if that intelligence community were to be handed over to a Government that was authoritarian. When I see some of the things that some of our party leaders are saying at the moment, I do not believe that they could be enacted in this country without authoritarian measures. To think that this perfect machine that we are constructing here, and that I am saying to you should be allowed to interfere with people's private rights, should be laid at the hands of a regime of this kind—I am talking particularly about UKIP—I find extremely disturbing.

So yes, privacy is not absolute; security is absolute. Certainly, people behave in such a way that their private lives should be, if necessary, lawfully investigated, but all this is predicated on our

adhering to the European convention on human rights and on our having a liberal democracy. Of course, the Security Service Act 1989 makes that entirely clear, and I am a strong believer in the Security Service Act.

Q4 Mr Howarth: To follow on from the question that Hazel asked, if the right to privacy is a qualified right, most people would agree that, for example, child abuse, national security and organised crime are clearly exceptions to that. Does Charlie Edwards think that that is the complete list, or does he think other things should be added to that list?

Charlie Edwards: It is difficult to answer the question as to whether it is a complete list, given that our ideas of what privacy means evolve as technology does and will do so in future. To answer your question, I come back to something that David said, which is that the world has changed. How has that world changed, given that one of Sir Ming's family is busy on Match or eHarmony or Tinder—apps that you can download to find a girlfriend? What does privacy mean in a surveillance society, which I believe we are in, although there are questions as to whether that is benign or a threat to members of the public?

There are three key actors in this surveillance society. There is Government and local government. To give you one figure, there are approximately 6 million CCTV cameras now in operation in the UK. There is, of course, the data industry. If the Committee has not read it, I recommend the latest edition of *Wired UK*, which has on its front page, "The data industry is selling your life". So, on all the points that Sir Ming raised, I do not think we quite understand—we, the British public—how much of our data is collected by private industry and how much is then sold and traded on our behalf, often without our consent. Partly there is a responsibility on the individual to agree to those terms and conditions, which one does, but I am not entirely convinced that the British public really understand.

Then there are citizens, or consumers, or individuals themselves, who are busy using their smartphones or the internet. To give you some figures, there are 10 million new photos uploaded every hour on Facebook; 800 million monthly users of Google's YouTube; and in 2012 Twitter saw approximately 400 million tweets a day. So when we talk about privacy, we have to first try and understand that as individuals and as a broader society we are going to have very different views of what privacy actually means. That is generational, clearly, but it is also in terms of location, too. The idea of privacy in London, for example, where you can literally be tracked by a CCTV camera from the tube station to your place of work, and on the tube and via your Oyster card, is going to be very different from a perception of privacy for someone who lives in a rural community. So I think there is a geographical argument to make. But there is one point—

Mr Blunkett: It is safety from cows, I have discovered.

Charlie Edwards: If only they could be tagged, which they probably are these days. There is an important point here around the segmentation of society. We use the British public very easily to describe what we are all thinking without going into some of the nuances of what people expect privacy to be today. There are some very good pieces of work that I would be delighted to share with the Committee from think tanks such as Demos, from the likes of Big Brother Watch and from Deloitte and PWC, who have at least now tried to understand what parts of society are more likely to give their data and why. There are five—

Q5 Chair: May I encourage you to bring this answer to a conclusion and to try to bring in your other points in subsequent answers? We have a lot of business to get through.

Charlie Edwards: You have non-sharers. You have sceptics. You have privacy pragmatists. You have value hunters. You have enthusiastic sharers. Those individuals, those groups within society, have very different views on whether they should share their data and why. So I don't think we can just assume that society has one idea of what privacy is. Actually, people will trade their data

if they see benefits and, coming back to your question, those benefits are obviously national security and public safety.

Chair: Thank you very much indeed. That has been a very good general introduction. Could I invite our witnesses to give reasonably succinct responses simply because of the volume of work that we have to get through? That has been very helpful. We now want to move to the heart of our inquiry and questions of surveillance and intrusion. The next section will be on targeted intrusion where the agencies under law seek to find information about specific individuals.

Q6 Dr Lewis: We are now going to deal with the easier end of the spectrum before we home in on the grey areas. What I am talking about in posing the next couple of questions is the circumstance where the agencies have specific intelligence that an individual may pose a direct threat to the UK. I should like to ask members of the panel, perhaps beginning with Rebecca Hilsenrath, whether you consider it is proportionate and appropriate for the agencies to investigate such an individual and for such an investigation to intrude on the privacy of an individual where there is specific evidence that they may pose a threat?

Rebecca Hilsenrath: The position of the commission is that we regard the surveillance and investigation of an individual, where there is a targeted operation and there is a suspicion of activities in relation to a threat to national security and so on, as being proportionate. Remarks have been made earlier in relation to the European convention on human rights. Lady O'Neill talked about balance. But article 2 is not a qualified right and we regard it as just as much our role to promote and safeguard it as to promote and safeguard article 8. We have other points to make in relation to the regime that supports that targeted investigation in relation to authorisation and so on. That may come later in the conversation. I am happy to stop there.

Q7 Dr Lewis: Can you just explain the reference to article 2 for the benefit of the Committee?

Rebecca Hilsenrath: Article 2 is the article that protects the right to life. That obviously underlies a lot of the work in relation to the protection of national security.

Q8 Dr Lewis: Does anybody disagree that it is proportionate for agencies to use intrusive measures in a case where a specific individual has been identified as someone who possibly poses a threat to the security of the UK?

Mr Blunkett: There are two provisos. One is obviously what authorisation has been granted in relation to those who are associated with, and therefore might be a means of identifying or reaching, that individual and, secondly, how much trawling takes place to find the necessary information—the data—or even identify where the individual is. The head of GCHQ gave a not terribly insightful interview to Charles Moore at the weekend, and talked about finding needles in hayfields rather than haystacks. The rub here—it is the easy end, because we would all accept that this is an area where we want our security and intelligence services and counter-terrorism police to be able to act—is how much of the rest of the hayfield we go through in order to reach them.

Q9 Dr Lewis: We will be coming to the wider collection of searching for needles in haystacks or hayfields, but we are not there yet.

Mr Blunkett: Okay. I give in, in that case.

Q10 Dr Lewis: Well, that's a first. We just want to consider where there is actually already specific evidence which has identified an individual as suspect in this respect. Finally, I would like to ask members of the panel whether they consider, if it is proportionate to conduct investigations of this sort, that the agency should be able to do any or all of the following: intercept the person's

communications, follow them, eavesdrop on them or any other of the intrusive surveillance activities with which we are all familiar. Perhaps Baroness O'Neill and then Professor Glees will comment.

Baroness O'Neill: It is, in principle, acceptable that with authorisation, where there is suspicion, such activities should be undertaken. The quality of the authorisation and the degree to which it takes account of evidence is important in that. I think there are also two further issues. One is about breadth. That is to say, such an exercise may pull in data relating to individuals associated with the suspect whose privacy also matters: family members, colleagues and so on. I think there is an issue about the retention of data that proves in the event not relevant to the issue, and its destruction if it is not relevant.

Professor Glees: A very brief answer to your question is yes, I think this kind of surveillance is entirely acceptable. I would just make the point—I disagree with my distinguished colleague here on the left, Lady O'Neill—that we do not live in a surveillance society. If we did, you would not need to ask that question. We live in a society in which a lot of data is collected—again, as has been pointed out, by Amazon and people like that. We are talking here about targeted interception of people who may want to do us harm.

I know you have been a target of the Stasi yourself. People often say, "This is a kind of Stasi activity." In 1989, one in seven East Germans worked for the Stasi. There can be no meaningful comparison. Even if the director of GCHQ gives a somewhat vague interview to Charles Moore, which I have not read, there can be no comparison between what GCHQ does and what the Stasi did. Even President Obama said it was meaningless.

Q11 Mark Field: Arguably, you could say that there is a comparison, if not in terms of the numbers of people of involved, then because of the internet. The sort of thing—eavesdropping, opening of post and the like—that might have happened in post-war East Germany would have been superseded, if that regime had continued to this day, by internet communications, which are arguably more intrusive than some of those traditional techniques. Would you accept that we are living in a very different and potentially much more intrusive world? Do you understand some of the concerns that individuals have about that sort of targeted intrusion?

Professor Glees: I understand the concerns, but I think they are totally misguided. Just because *The Guardian* newspaper—abusing what Edward Snowden actually said, because Edward Snowden himself did not say this—says "We are all under surveillance," it does not follow that we are all under surveillance. However, if this meeting were taking place in East Berlin in 1989—of course it couldn't have done—I would not have been able to say that. Everybody seriously was under surveillance, and not just East Germans; your distinguished colleague Dr Lewis was under surveillance. We have to distinguish between the ability to collect electronically transmitted communications and their decryption and interception. The two things are not the same. I accept that it is much easier for people to communicate electronically—we all do it, all the time—and it is also easier to collect that data. But it does not follow that collecting the data leads to it all being decrypted and acted upon. That is an absurd proposition.

Mr Blunkett: In practical terms it cannot be, but there is one proviso to what has just been said. That is the way in which we need to protect ourselves from the collateral impact that occurs, even where we are targeting, because there will be other people who are drawn into this. When you grant warrants, as I had to do, for obvious reasons you are always mindful about whether other people are being drawn into the net.

Charlie Edwards: I want to come back to the surveillance society point. Professor Glees disagrees with me, but I take Mr Field's point. The fact is that there are organisations that are very busy identifying and collecting our data and then using it. That is private industry—they are monetising our data in order to sell us things, or, at least, to understand what we are doing so that we have some benefits in the future. That is very different. The historical concept of the surveillance society that Professor Glees has just given you about Germany and the Stasi is very different from what people would think about today. Therefore what we require are the right safeguards, the right

oversight arrangements and the legal framework to ensure that from a government perspective that is all done legitimately. There is a difference there from private industry.

Mark Field: But within the concept of that—though I think you are right about the monetisation and that people think there are financial benefits—can consent be implied, or does there have to be direct consent from an individual for that privacy to be targeted?

Charlie Edwards: The issue of consent is extremely problematic when it comes down to the way that we buy and procure services today in industry. There are the terms and conditions that those companies set out, which they would say are very clear, that you are providing consent for them to take your data and to use it and trade it. However, consent today in an information age is very difficult to understand. Therefore implied consent becomes the issue of the day. I am not convinced that members of the public really understand it.

Lord Butler: Of course, when we are talking about targeted intrusion, it requires to be warranted. At the moment I do not want to go into who should issue or approve the warrant, but what the criterion should be. Intelligence is not always clear-cut or 100% reliable, so this targeted intrusion has to be considered in cases where there may just be reasonable suspicion. I want to ask the panel's view on whether reasonable suspicion is an adequate criterion for targeted intrusion. Since David Blunkett has had to issue such warrants, may I start with him?

Mr Blunkett: It is a question of what that suspicion leads you to believe they are likely to do. The easy bit was where you believed they were involved in a conspiracy to carry out a terrorist act of one form or another and where there was organised criminality that involved weapons. Those warrants were easier to attest then where you had the suspicion that people were organising in a way that led to the belief that they would at some point be in a position to carry out that activity. That is why—and this is the paradox—we actually took greater care, with much greater safeguards, including the commissioners testing what we had done, with those about whom we had greater knowledge and suspicion, than we do with the use of RIPA for police authorisation.

Q12 Lord Butler: Does any other member of the panel want to add to that?

Professor Glees: If I may say so, I am not talking about the sorts of things that Charlie Edwards is talking about. My interest is totally in the delivery of intelligence-led security policy; it has nothing to do with what John Lewis or Amazon do, and I would not want to comment on that. The fact that people commit crimes in private does not mean that they are not crimes; in fact, most people commit crimes in private if they possibly can, so that immediately, for me, blows the argument for privacy out of the water.

However, under no circumstances, in my view, should intelligence-led activity be used as a form of social control. That comes back to the European convention on human rights and the decision of the Conservative party that if it wins the next election, it will seek somehow to withdraw. We all know what UKIP thinks about the European convention. It would be only too easy to use all the things that we are talking about in a completely different way if the political complexion of this United Kingdom were different. It would be all too easy to use it as a form of social control. So privacy is not a barrier, but lawfulness is absolutely critical.

Baroness O'Neill: Obviously, there are lot of difficult things in here, but I would say that one of the things that one cannot do is to set out in the abstract the criteria that should be followed in moving from suspicion. I would put the emphasis a little more on the word "reasonable". I think a case has to be made, and that is why robust processes of authorisation and subsequent oversight seem to me the key to this. One cannot simply say, "I had a reasonable suspicion."

I have a separate comment to make, but it links in. The metaphor "surveillance society" is one that invokes obsolete technologies, such as cameras—although they still exist. Most identification and most work is inference, not looking, at present. Most of the discovery of what people are trying to keep hidden happens by inference, and that has happened ever since we have had detective stories; we know about that. The problem that this Committee and others face is that it is possible, using big

data, data-mining and analysis techniques, to draw inferences that were not feasible in the past. The Stasi would have loved it, but thank God they did not have it.

Q13 Chair: Let us move from targeted intrusion to the area that has perhaps given rise to the greatest expressions of concern from some quarters: the question of what is often referred to as bulk interception, where information is made available from a very large number of people in order to enable the agencies to identify whether there is useful information from some of the large number they have intercepted.

Lord Lothian: We have already begun to stray around the periphery of the hayfield where the haystacks are, and this is where we begin to look at them rather more closely. I just want to try to establish whether there is a consensus on various points before we go deeper into the hayfield. I think we all agree that the use of targeted techniques can be justified where there is a specific and acceptable reason for doing so—whether or not that is reasonable in the light of what Baroness O'Neill has just said—but I wonder whether we accept that in order to get to that stage, the agencies have to find those individuals in the first place, and that is where the analogy of the needle in the haystack comes in. Do the witnesses recognise that before the agencies can use targeted techniques, they have got to go out and find the individuals in the first place, and to do that they may have to delve into communications? They often do not know who they are looking for and they do not know what communications they need to collect, so there has to be a wider collection of information on communications data. Is that an accepted point from which we can move further into the hayfield?

Charlie Edwards: We began the session by talking about changes in society and how much data is produced. For me, at least, it follows that given the vast amount of data there is, the agencies are caught in a bind. In order to find the individual or the piece of data that will be useful for an investigation, they have first to take a volume of data. They then have to filter that data and then, and only then, can they target it through a warrant.

That to me is the fundamental challenge that the agencies face today. It is the fundamental challenge that the Congressional Research Service identified in 2000, prior to 9/11: that the increase in data will mean that the agencies will have to find a way to reduce the volume of data—filter it—in order then to find, in this case, haystacks and then the needle. That all has to be done under a legal framework, but it does then challenge our perception of what is proportionate and what is necessary and that is the debate that the ISC and others are having to have.

Q14 Chair: Could you indicate your personal view as to whether, in a democratic society, it ought to be acceptable to have what is often referred to as "bulk collection" in the circumstances you described?

Charlie Edwards: I do not really like the word "bulk", but I accept that we have to use it. The volume of data is such that I cannot understand personally—I am not a technical guru on this—an alternative to identify the relevant data, given the vast amount that we have to source and look through today.

Q15 Hazel Blears: I wanted to explore this a bit more closely. There is a broad acceptance that the threat to the country means that we need a proportionate response. I very much liked Baroness O'Neill's first analysis that this is not necessarily about balance, but about saying, "There is a right to privacy and then the way in which you have constraints on your intrusion depends on your legal framework," which I thought was a new way of putting some of these issues. However, when you come to bulk collection, there is a matter of principle on which I would be interested in your view.

Bulk collection is not about suspicion or targeting; it is about saying, "How do you develop your targets and look for patterns of behaviour so that, in effect, you are in advance of the threat?" In those circumstances, is it legitimate to have the haystack and go searching through bulk data? Charlie just said that, because of the amount of data, it is because there is no alternative to that. I was

wondering, however, whether you think there is a connection between the level of threat and how much you are prepared to have this mining of data to develop targets. For example, if there was an imminent danger of attack, would the balance—or, if you like, the constraints—change, depending on the intensity of that faced threat? Is this an academic discussion, or a practical one?

Baroness O'Neill: It becomes very practical. The difficulty with which we all have to wrestle is how to tie it down practically in a way that is adequately human-rights compliant. I would say that we have not helped ourselves, or perhaps the past legislation has not helped us, because we are relying on a couple of distinctions that are probably technologically obsolete: one being between external and internal data; and the other being between communications data and content.

The notion of content is reasonably clear in other contexts, but technology means that there is now so much communications data that a great deal of content can be reached by a matter of inference. As the contemporary information society is not a surveillance but an inferential society, we have to realise that inferences will be made from data.

A very interesting point to explore is whether there should be stricter standards for some organisations than for others. Charlie Edwards has already pointed out what the commercial sector does under the banner of notional consent, or bogus consent, if you will: tick and click, and that was your consent. Perhaps it would not be seemly for the state to behave in that way, but we must find a way in which, where it is seriously intrusive, people do not rely on tick and click. That is the difficult thing. Of course, we have got to be able to reach the stage where you have an individual to investigate. The early stages of investigation cannot presuppose that you have fingered the person.

Q16 Hazel Blears: You accept that there is a role for target investigation and target development before you get to the intrusive surveillance on your reasonable suspicion, but do you believe that privacy concerns bite at the point of collection of information or of interrogation?

Baroness O'Neill: I think they bite at the point of the interpretation of data, although that is a rather weaselly way of putting it. Most of what is collected under the vast array of the things that get called communications data—I accept that is an unsatisfactory term—are susceptible to various sorts of communication and inference. Going back to article 8, what we are really hoping to protect is people's families, correspondence and personal privacy. I believe one should look carefully at what is done to the target of surveillance. Frankly, if people were to look at my shopping behaviour, they may get bored but they would certainly not be the wiser.

Q17 Hazel Blears: David, you raised an important issue in the House and subsequently about the issue of passive reception, which is when we receive information that we did not deliberately set out to collect in a bulk way. There appears to be a lacuna at the moment, in terms of authority and cover. Do you want to say something about that?

Mr Blunkett: I am much clearer about how we need to update the legislative framework, and therefore our ability to retain necessary data, in different and changing forms. We must update the accessibility of the data and the restrictions placed on it, in terms of who can have access to what and why. I do not have a simple answer to this, but I am more concerned about when it is not the interrogation of the data with a specific eye to finding out things that are flagged up automatically now—GCHQ is expert at finding the kinds of data that would throw up the potential danger or the route to be taken to protect us—but when it is supplied externally, where there is no authorisation and where we have not put in place protection. That issue was thrown up in relation to the NSA. We are in a global environment par excellence, in terms of cyber, and we need to return to that issue. However, it is difficult; if it were not difficult, we would have resolved it.

Q18 Hazel Blears: I want to raise one supplementary issue. Nobody has dealt with my question about whether, if the threat intensifies, there is a corresponding—

Mr Blunkett: But it is the activity levels, Hazel, rather than the fundamental question of whether we change our practice and whether we have the capacity to do that.

Q19 Hazel Blears: I am trying to pursue this so we get some things on the record. I notice that Baroness O'Neill said the point of interpretation, rather than the point of interrogation, was the point at which privacy concerns bite. I think that is perhaps not the clearest way. What we have got here is a distinction between intrusive surveillance, where you have reasonable suspicion, and bulk collection, where you are developing targets. That information is not examined unless there is a specific search, in terms of criteria, to ascertain the patterns of behaviour. I am trying to find from you whether you think it is justified to have bulk collection for target development, looking at patterns of behaviour, subject to constraints—we will debate the 8(4) warrant system later. Do you think it is acceptable to have that bulk collection, which is not interrogated randomly, but is interrogated to ascertain threats? What is your view of the spectrum about where you can go?

Professor Glees: May I answer your very important question with a categorical yes? The reason that Sir Iain Lobban talks about a hayfield rather than a haystack is to make the point that the data is not, as in a haystack, cut and collected and formed. It is, as in a field, unformed and it is out there. It is penetrating that field in order to search for intelligence. What we did at Bletchley Park, which is about 15 miles away from the University of Buckingham, is rightly regarded as Britain's greatest ever intelligence success. What was that success based on? It was based on the interception of electronically communicated data. The volume may have increased but the principle is still the same. I seriously think we have to give our intelligence and security community the tools it says it needs, and rely that they will deal with it lawfully.

Sir Anthony May's report should be required reading for every journalist. We have seen that the behaviour at GCHQ and other agencies is virtually 99% to 100% lawful. I do not think anyone could say Sir Anthony was a whitewasher. The real answer to your question, Ms Blears, is that this is about public understanding, public trust and your job in providing oversight. I think the vast majority of people in this country, when they are not being misled by *The Guardian* newspaper and Snowden, would be perfectly satisfied. We live in very dangerous times; we have to let our security community go after those people who want to do us harm.

Q20 Hazel Blears: Are there any other views that do not entirely subscribe to those of Professor Glees?

Baroness O'Neill: It is important to attend to the false positives in this—namely, the people about whom you might get a case or draw an inference that there was a reasonable suspicion. Some reasonable suspicions turn out to be misplaced. One does need, within the system of authorisation and oversight, some explicit recognition of what will be done in the case of misplaced suspicion and which data will be destroyed. It is, I take it, a very traditional part of police work that they rule out a suspect. Now that so much data is retained, I think it extremely important to be explicit what will be done in that case.

Mr Blunkett: In one very straight example, the Investigatory Powers Tribunal needs to be vamped up considerably. People need to know a lot more about it. It needs to be much more transparent and able to demonstrate that it is worth having.

Q21 Sir Menzies Campbell: "Reasonable suspicion" is an expression and a standard which is familiar to all of those who are either responsible for apprehending criminals or, indeed, who practise criminal law. I can be arrested on the basis of reasonable suspicion but it does not necessarily mean that I will ever be charged or convicted, so I rather support the view that Baroness O'Neill was expressing. I may have misunderstood you, David Blunkett, but I thought you suggested that there may be different standards of reasonable suspicion where there is a more serious outcome. I would politely take issue with that.

Mr Blunkett: I am not advocating it; I am saying that is how we perform.

Q22 Sir Menzies Campbell: In that case, can I test you and perhaps support you in a rather different way, if you are willing to be supported? If it is proportionality and necessity, that is quite different because proportionality raises the question as to whether it is a demonstration outside Parliament, at which someone might steal a policeman's helmet, or whether it is putting a bomb in Victoria station in the middle of rush hour. Do you recognise that reasonable suspicion is subject to the kind of criticism I was making? When it comes to proportionality and necessity, how you practise it may be extremely different.

Mr Blunkett: To clarify, I was trying to say that we are very methodical and, I think, correct in the way we deal with authorisation for the targeted and very serious threats to our life, wellbeing and the economy and society we live in. That is, Ministers of the Crown, Home Secretary, Foreign Secretary and, in the past, Northern Ireland Secretary have had to provide those warrants and go through them. They are returned on a three-monthly basis for re-authorisation.

When it comes to surveillance and the way in which we intrude on suspicions at a lower level, until recently it was a superintendent in the police who did it. I think they have just revamped that to assistant chief constable. There is an HMIC report out today about secret policemen, if you want to call them that, that indicates that there has been a tightening up, and that it has to be an assistant chief constable, but very many are not trained at that level to do it. This is not necessarily the remit of the ISC, but we do need to get it right. Otherwise we are most protecting the interests, freedoms and civil liberties of those we suspect the most.

Q23 Dr Lewis: I want to come back to the point about the legitimacy of collecting or retaining the hayfield in the first place. A number of submissions that have come in from organisations and members of the public have so highlighted the dangers of the authorities fishing in this huge pool, to change the metaphor slightly. They say in that case it is quite wrong for the pool to be retained, and that the only inquiries that the security services ought to make are based on specific individuals about whom they have already some hint or tip-off. I would like to get from you whether you accept the distinction between retaining this huge database and then interrogating and examining it; or whether any of you believe that the danger of a fishing expedition is so great that it is wrong to retain the database in the first place.

Charlie Edwards: It is an interesting distinction. The first point concerns how long in this case GCHQ retains that large database.

Q24 Dr Lewis: With respect, that is not the first point. The first point is whether they are entitled to retain it for any length of time at all.

Charlie Edwards: We have already had a discussion about the volume of data and the collection of data and the fact that there has to be a process of filtering, which could be called mass volume reduction, for want of a better phrase. That process has to occur. When that process is occurring, I assume they are taking that data, filtering it and discarding any data not relevant to their investigation. From there they are identifying the relevant individuals or data with selectors, or whatever it may be. From my point of view, I do not see how they can go through that process without retaining that data for a period of time. I do not know the precise details of how long they are able to retain that data, but I assume they will have days if not months they can then move that across.

Q25 Dr Lewis: Some people argue, for example with the argument about communications data and whether companies should retain that at all, that it is wrong to retain the database for any length of time. Does that argument find any support from the team we are inviting to comment today?

Professor Glees: I think this critical question has to be tackled head-on. We hear the same sort of thing about retaining DNA, as if the retention of DNA were the enemy of justice. It is quite the other way round. The retention of DNA enables many people who have been wrongly convicted to gain their freedom. We should be very much in favour of that.

Focusing particularly on internet-generated data, I do not think that there is any decision more harmful for the development of the free and liberal society than the right that Google gives for people to remove past entries about themselves. We often hear that people like me support some kind of Orwellian nightmare. The Orwellian nightmare is removing the facts about the past.

My final point is that any intelligence community relies on its records. One of the worst things that MI5 did was to destroy hundreds of thousands of records 10 or 14 years ago. That was utterly absurd. Records are absolutely key and if the records are electronic records they then become key. The idea that they should be destroyed is not only a waste of time but also terrible security and intelligence practice. Of course, all this has got to be done lawfully, with a proper warrant. We have heard from David Blunkett that maybe round the edges this needs to be tightened up, but there is no great concern about falling over backwards to accommodate the views of libertarians in the Conservative party and in the Liberal Democrat party, and also now in UKIP and in Liberty. These assertions are made on the basis of a complete lack of understanding. None of us would dream of going in to our GP surgery if we did not feel confident that our doctor had our records.

Mr Blunkett: Anthony is making me feel like a real pinko.

Chair: I am sure you will rise to the experience.

Q26 Lord Lothian: One of the things that has come out of our conversation so far is an acceptance that the advent and development of the internet over the last 20 years has changed society. I wonder whether the core principles relating to privacy across communications still apply across the whole range of communications, or whether there is now a need for a higher or different level of principle in relation to internet relations, and if so, why?

Baroness O'Neill: I think it is very difficult in that in the European Union, as well as the convention right, we also have the Data Protection Directive, its implementation in the Data Protection Act here and prospectively the Data Protection Regulation. All of these take the view that if you can infer the identity of somebody—if it is possible to infer when the data controller or any other person reads the directive—then the data are personal data. I believe that if we want to have effective protection of the right to privacy, we have to refocus ourselves on what really matters to people in matters of privacy. The convention is not stupid in talking about the home, the family and the correspondence, but because we now have these influential possibilities that multiply all over the place, it is indeed tempting to think, let's dig up the hayfield. That is an illusion because the hayfield is not solely, nor even perhaps mainly, under the control of Governments. The hayfield is out there all over the place and the major communications providers have access to huge amounts of data. I think we need to back pedal a little bit and think about what privacy is for and how could we best protect it, with a positive set of questions, rather than, as it were, getting in downstream where the way the stream is flowing has been structured by some very difficult distinctions about internal and external communications content.

Mark Field: One of the biggest concerns that some of us had about the Snowden revelations was this sense that there was almost an irresponsibility from *The Guardian* in not recognising that a lot of intelligence is a jigsaw of particular bits of information that are known. One of the suggestions from one response to this inquiry is that the circumstances around the reading of an individual's communication should be made much more public and the Government should be much more open about this. Do you share my concerns that that will give rise to knowledge of the modus operandi that intelligence and security services utilise, which could allow a lot of terrorists to have a clear understanding of exactly what is going on? Arguably, Snowden has already done that to quite an extent—elements of some of the operations come into place. I suppose what I am really asking is, I have posited an issue and a problem that I hope most of you will agree is there, but do you have any

solutions for this apparent paradox? There is this demand that individuals should be given more right to understand what is going on, but in so doing we are potentially making ourselves less collectively safe.

Professor Glees: I think we are making ourselves and have made ourselves less safe. Things that I have written have often reflected what I have picked up in the work that I do, and the people I speak to may not be able to speak out as I may do. The Government have behaved wrongly over Snowden. His helpers had access to our most sensitive official secrets and Mr Miranda should have been prosecuted—I have argued that. But, from the vantage point of an intelligence community, it is by no means a simple thing, because on the one hand they want people to communicate electronically, because that is how they derive their intelligence, but on the other they do not want to be seen to be undermining the privacy of people who are behaving completely lawfully.

As I understand her, Lady O'Neill says that we have to find out what really matters to people in terms of their privacy. That applies if you are a perfectly ordinary person, but if you are a terrorist, for example, or a paedophile, sex trafficker or drug dealer, what really matters to you is not letting anyone know what you are doing. A right of privacy for one set of individuals cannot apply to other sets of individuals. The internet, which is currently unregulated, needs to be regulated. If it was regulated and people knew that it was, they would think more positively about their privacy. However, of course, the flip side of that would be that if it was more regulated, there would be less intelligence.

I am in no doubt that people have been alerted. Look at the way in which on the one hand, with ISIL, we do not know where these people or those people are, but they are busy using the internet to communicate their propaganda to us—that shows the complexity of it. I am in no doubt that intelligence is going to be much harder to gather from the internet in future, because people have been alerted. If they had thought about it for five minutes, they probably would have sussed out that it was going on. They have now been alerted, and the intelligence community is going to have to go back to older forms of gaining intelligence.

I think your point is a very good one, but it is also very, very complicated and will take many years to work out. I notice that Sir Tim Berners-Lee, a passionate internet libertarian, has said more recently, "No, some new kind of regulation has to be introduced."

Mr Blunkett: Just to pick up Mark Field's point directly, I think that earlier we felt collectively that the word "balance" was not quite right, but in this context I think it is. We were on the one hand trying to protect ourselves from knowledge that would undermine the very purpose to which we are engaged, although I think that the most sophisticated of our opponents actually have a pretty good idea of what we can do—in fact, sometimes we are trying to catch up with them.

The second, equally important, element is the reassurance and consent of our own population. That is in the essence of a free democracy. It is therefore important to ensure that people feel comfortable and know enough about what we are doing to feel that it is in their interest. That is why I said in my submission that sometimes—I know why we do it because I did it myself as Home Secretary for three and a half years—we have got to try to sophisticate "We can't tell you anything because it might be of danger." That starts to undermine confidence and consent, because it is real old-fashioned paternalism—it is, "We know, but you mustn't know."

Chair: We will be dealing with transparency issues later in this sitting, but we have two more questions before we move on to the next section, the first from Ming Campbell and the second from George Howarth.

Q27 Sir Menzies Campbell: Provision is made for the use of the powers available to the security services in relation to the kind of threats that are more currently in our minds, but the issue of economic well-being is also raised. How far is that justified and how far is there a sufficiently clear definition of the circumstances in which interception may be justified for that purpose? Is the present law adequate, should it be stronger or, indeed, should there be a relaxation?

Baroness O'Neill: I will have a go at that. I have been struck that, despite the fact that we have a uniform privacy regulation in the European Union, there are very different views about what is private in different European Union states. In a couple of the Scandinavian states, everyone's income tax return is online for the public to look at. It strikes me that that must be a very salutary although not, perhaps, a very popular measure. It seems that the economic impact of having, as we have in this country, the view not merely that income tax matters are private, but that they are very exceptionally private, is striking, has its costs, consequences and maybe its benefits. There is no "bright line" here. When one looks at economic espionage and technical espionage as well as the privacy of the income tax return, one can see that there could be, compatible with a society where government is by consent, a variety of solutions.

Q28 Sir Menzies Campbell: Well, we have some experience, from the point of view of MPs' expenses, of the kind of illustration that you give.

Baroness O'Neill: Indeed.

Q29 Sir Menzies Campbell: I think it is generally accepted that there is a large volume of activity in this country on behalf of countries that might previously have been, shall we say, in a more aggressive posture that is less to do with whether we are developing hydrogen bombs or things of that kind and more to do with whether or not our commercial secrets can be trawled. I wonder the extent to which you think that that is something that we should be using this kind of legislation to try to protect?

Professor Glees: If I may, very briefly, comment. The Security Service Act 1989, as you know, specifically talks about the duty of the security service to protect the country from activities designed to undermine the economic well-being of the United Kingdom. That is necessary in a precise way when it comes to the use of the internet—one reason that I do not think it should be entirely unregulated—by people who are stealing our economic secrets and undermining us in that way. Of course, there is another aspect that will put our security and intelligence community in a very difficult position. If Britain was to leave the European Union, for example, many people would think that would seriously undermine the economic well-being of the United Kingdom. After all, the same argument was made in the case of the Scottish referendum.

Q30 Chair: This really has to do with many different things so the EU will have to wait for another day.

Professor Glees: I know but all I am saying is that the Security Service Act 1989 does not need changing.

Q31 Mr Howarth: This question is about effectiveness and how you provide evidence that shows that one kind of intervention is justified. There is a real dilemma. Some would argue that there is not sufficient evidence to prove that interception techniques are effective. On the other hand, the agencies and others might argue that to provide that evidence, they would have to reveal a lot more about techniques than would be wise, in terms of those who want to do harm knowing what their capability is. There is a variation on that, which I will throw into the pot—some people have argued in written evidence that they have submitted that even if there is a risk of some incidents, the principle of not authorising interception is so strong that that is a risk worth taking. The difficulty we all experience is how do you have that debate? What are the terms of that debate and how do you produce evidence that might convince people of the necessity of some forms of interception?

Charlie Edwards: May I have a go at answering that question? I think it will continue to be a perennial problem. It comes down to the confidence and the trust we have in the mechanisms for oversight and accountability, be that the ISC or be that the other Select Committees that have a responsibility for overseeing the relevant Government Department—Home Affairs Committee,

Foreign Affairs Committee and so on. There are also the independent commissioners and the regulator. There are lots of different institutions that have been created in order to ensure the relevant oversight and accountability. However, to the broader public that probably looks like a mess of organisations, which may not necessarily help them navigate through this information. It may not be clear that they should go to the independent commissioner on communications or, indeed, on interception or intelligence. It might not be clear whether they should look to the ISC or to the Home Affairs Committee.

I think the challenge here from the public's perspective is not necessarily whether or not interception is effective because we may be able to see that in some cases, in the summaries of those cases, which can be got, or indeed from websites of the relevant police forces who wish to demonstrate how an investigation went well and what they used—Operation Crevice is a good example of that. It is rather whether they have trust and confidence in the institutions that provide that oversight and accountability in the first place.

Mr Howarth: As a supplementary to that, and the others might care to comment on this, one criticism that could have been made of this Committee in the past, for example, was that we were a bit in the shade, we were not necessarily outward-looking, we did not engage with the public as much as perhaps people felt we should have done. This is a public session today, we have had one previous public session and the intention is that we will be more out in the open. Some of the other parts of the oversight mechanism rarely—

Chair: George, we are coming to oversight in about 10 minutes time. Please come in then; I think it will be more appropriate.

Mr Howarth: Sorry. I will leave it at that.

Chair: We will come back to oversight. We have got just under half an hour of the session left and there are several important questions to raise. The first is the question of the legislation under which the intelligence agencies operate. I would like to ask, if I may, two related questions to you on this. RIPA, which is obviously the main legislation, has been described as "an analogue law in a digital age." I would like any observations you might wish to give as to whether RIPA itself remains appropriate or whether it needs reform in any substantive way. Linked to that, even if the law under which the agencies operate does not need to be changed, does the way in which it is interpreted by Government or by the agencies themselves need to change? Sometimes it is suggested that there is too much flexibility, that it is too loose and it allows agencies to do almost what they like and still claim that it is lawful. We invite your comments on those matters.

Baroness O'Neill: I must say that certainly the Equality and Human Rights Commission has come to the conclusion that RIPA is time-expired. It needs to be reformed and, of course, there is agreement in that DRIP expires in December 2016 so there will have to be new legislation. That is surely an opportunity to get greater clarity about the authorisation mechanisms to make it clearer for the public. I very much agree that a great deal of this information about how it is done can perfectly well be in the public domain. They do not have to know how which bit of surveillance was authorised, but they can know that there is a process for authorising it, and equally—I hear that we are coming to oversight—they can know that there is a process for checking that what was authorised is what was done.

Q32 Chair: Just to be clear about what you are suggesting, you say that RIPA needs oversight, and it needs to be replaced or renewed—

Baroness O'Neill: RIPA's successor needs to have simpler and clearer structures for both authorising surveillance or the collection of data, and for the discarding of information, to make it clear that both the authorisation and the subsequent oversight or audit function need to be separate, clear and independent.

Q33 Chair: Would other colleagues either agree with, or in any way disagree with, what we have just heard?

Mr Blunkett: I don't think the intention is simply to start from scratch with RIPA. The necessity to update is obvious. I was not responsible for oversight of the passing of RIPA in 2000, but I was responsible for the introduction of the regulations, which proved to be a great deal more difficult. I think I am on record as saying that one of my Ministers had a go at that and my son, who had just done a computer science degree, phoned me up and said, "This won't do, Dad", and he was right, so we had another go at it. And in 2006 we saw the need to revise it; we have seen it again since, because of erosion or dilution, or because people are pushing the boundaries all the time.

I say for the public record that the Regulation of Investigatory Powers Act 2000 was supposed to regulate and confine, rather than open up. The intention was to define and confine, and I think you need to get back to that, while accepting—as we have during the course of this morning—that section 8.1 and, to some extent, sections 8.4 to 8.6 have been working. What we need to do now is to bring the Act up to date and ensure that the oversight mechanisms, including returning to the Act in each fixed-term Parliament, ensure that people have confidence in the Act.

Charlie Edwards: It is worth pointing out that RIPA was introduced in 2000—pre-9/11—and it was there to change some of the points in the Interception of Communications Act 1985. So it was attempting to address a problem that had been identified by Government.

I do not think you can read the legislation—even Sir Anthony May says you cannot read it—because it is pretty challenging to do so. However, the codes of practice are quite clear and Sir Anthony's reports are very clear. So, yes, the legislation may be impenetrable, but there are other ways of understanding RIPA. Clearly, if we are going to review RIPA—as we are, through David Anderson and others—it is to take into account the fact that we probably need to communicate what we are trying to do with this legislation, as well as getting the words on paper right.

Chair: Thank you; that is very helpful. Julian, I think you wanted to come in on the European convention.

Q34 Dr Lewis: Yes, indeed, so I will try to bring you, Rebecca, back into the conversation by referring to the European convention on human rights and the UK's Human Rights Act, which indicate that the interception of the content of communications is permitted only if three tests have been passed: that it is lawful; that it is necessary; and that it is proportionate. I understand that to mean that there must be a "lawful" purpose, which for the intelligence agencies means that it has to safeguard national security, including where that relates to economic well-being or the prevention of serious crime. "Necessity" means that the information being sought cannot be obtained by other, less intrusive means. "Proportionality" means that it must be no more intrusive than is justified by the purpose of the investigation and that it must consider the impact—as Baroness O'Neill mentioned in her earlier responses—it might have on the privacy of innocent people who are, as it were, collaterally involved. Do you consider that these three safeguards are sufficient for the purposes of those two Acts?

Rebecca Hilsenrath: I think our position is that the safeguards you mentioned, which come directly from the Human Rights Act and the European convention, are workable and appropriate, but we don't think that under RIPA they are effectively and consistently applied. You are correct in saying that they apply to systems of interception for targeted, warrantable data such as the content of individuals' communications, but this is not the case in relation to communications data or communications which are intercepted externally. The problem with RIPA is that it has been superseded by technological developments which have come latterly. This means that the lawful basis on which interception must be justified is inconsistent and, frankly, rather random in terms of whether a particular instance can be lawfully justified.

Q35 Dr Lewis: Could you just help us by giving one or two examples of the way, in practical terms, that, shall we say, ossification of the existing regulations has become apparent?

Rebecca Hilsenrath: I am not sure I can give you a specific example in terms of cases, no; but for us, it is about looking across the way the Act works and looking at the broad categories of interception, which are not consistently regulated.

Q36 Dr Lewis: To better enable the Committee to grasp the anomalies that are being suggested, can anybody else indicate where it might be a problem in concrete terms?

Professor Glees: I would like to answer that very briefly—and partly answer the previous question, because I think they are interconnected. I was strongly in favour of there being a new law on data interception a couple of years ago, but that Bill could not get through Parliament because of—again, where else but in Parliament?—libertarians on the right and libertarians in the Liberal Democratic party. I think that has to be looked at again, and I think one way that you get public confidence in intelligence collection and analysis is by being able to demonstrate that it is done lawfully, so I do think we need new Bills.

There is another aspect to RIPA. I am referring not to local councils checking up on people's bins—although I think there's some logic there—but to the increasing use by the police of communications data. Just this morning we are hearing about the grave public concerns—and I actually share them—about undercover policing in this country. If there were a greater use by the police of communications data, there would be far less of a need to have undercover policing. There always has been a need. We all know that police forces are rapidly wanting to expand their use of intelligence, and this should be set out lawfully, so that it can be done lawfully.

Q37 Dr Lewis: You are dissenting, Baroness O'Neill.

Baroness O'Neill: I am dissenting simply because I think that to pin it on a category called communications data is to preserve one of the things that has led to the problems with the current legislation. I remember on many occasions, when various legislation was discussed, we were told that communications data was just the where and when of phone calls or e-mail traffic. It is, of course, richly informative, and I think that that category may not be useful to us. Of course, you cannot forbid its use. Among other things, it is being used constantly and intensively by commercial companies for all sorts of reasons, and not only for reasons that are, as it were, internal to the company. For example, if you have a sat-nav, the information that tells you where the traffic jams are is obtained by monitoring other people's telephones as they get stuck in traffic jams. That is an example of a perfectly lawful use of communications data, but I do not think one can say that communications data as such are sufficiently uninformative and unintrusive that they can always be used—*[Interruption.]*

Q38 Chair: We will just pause for a moment until the bell stops. I am sorry, the bell obscured Baroness O'Neill's last word. What was your last word?

Baroness O'Neill: I forget what the last word was, but the thought was that "communications data" was not a sufficiently robust category to be something on which to build legislation and that one might need to go for a clearer view of which sorts of communications data are collectible and which are not, with what sort of warrant.

Q39 Lord Lothian: I would like to look more specifically at the interception of communications under RIPA. The written submissions made to us suggest that the use of RIPA 8(1) warrants is really regarded as necessary and generally acceptable; but in contrast, the same submissions have based questions about the use of RIPA 8(4) warrants and external communications. Obviously one of the main differences is that under RIPA there is a lower threshold for intercepting

communications involving a person or entity overseas—that is RIPA 4. I wondered what your views about this are—I do not know who would like to start.

Baroness O'Neill: If I may start with the thought that it is of the essence of communications nowadays that they are not located in any clear way, given that the servers, the cloud, wherever, are somewhere on earth—mainly, by the way, in the state of Washington; they have cheap electricity there. Therefore, the idea that you can draw a clear line between internal and external communication is now in question. I do not think one can expect to have a clear system that can be understood by the public and may gain their trust if one uses a distinction that has become fuzzy.

Rebecca Hilsenrath: I would add to that. I think we have a further concern that if, under a technological regime—which I am afraid I am too much of a Luddite to be able to specify—you were looking at the destination of communications, in terms of the internal and external divide, a laxer regime in relation to communications which were going outside the country might have a disproportionately burdensome effect on members of minority ethnic groups living in this country.

Q40 Lord Lothian: May I just add in the practicalities? You may then, Professor, be able to answer that as well. Obviously if the agencies are looking at individuals within the United Kingdom, they are more likely to have specific information to operate on. If they are looking at, for instance, terrorists overseas or spies overseas or whatever it might be, they may not be able to target it quite as accurately and they may need, therefore, to look at categories of communication rather than targeting specific, named individuals. If we do not make that distinction, in terms of the two warrants, how would you tackle this particular difficulty?

Baroness O'Neill: It would be one thing to target it in terms of the locations of persons. The location of communication seems to me an uninformative idea. Many of us use—*[Interruption.]*

Chair: Just pause for a moment for the bell, please. Thank you.

Baroness O'Neill: Many of us use Dropbox or other cloud data storage devices. Does that make all our communications external? I do not know the answer to that question and it seems to me quite fundamental. I may be in the UK, but I believe my data to be in the cloud, and I believe the cloud to be probably somewhere in the state of Washington.

Mr Blunkett: May I refer back to a separate but related issue that Hazel Blears raised with me earlier? GCHQ obviously are doing their job all the time with data from whatever source in whatever location. There is the related issue of how we handle data that we have not ourselves sourced and the impact that has on individuals in this country, where in other circumstances proper authorisation and oversight would exist.

Professor Glees: I would like to dissent very much from the view expressed by Ms Hilsenrath. The implication that, somehow, communities—by which I think she meant Muslim communities—in the United Kingdom would be upset if there were not this careful distinction made, is quite wrong for two reasons. British Muslims are as much at risk from jihadism as every other person in this country and I do not think that one should make any assumptions about what they may or may not feel about security. In my research I found that Muslim communities in Buckinghamshire regard the security service as an extremely important friend of theirs. I therefore do not think that that is right.

On a deeper point, one of the things that we are seeing in the world when it comes to, let us say, IS terrorism, but also communications, is that the distinction between what is home and what is abroad can no longer be maintained in its present form. Again, I would say that we need to have new legislation that recognises that. You can have people in this country who—wrongly, in my view—believe themselves to be better placed as citizens of the Islamic state. Equally, as Lady O'Neill said, we can all store or download data from other countries.

I therefore absolutely accept the point that you are making, Lord Lothian, about the two different ways of looking at data. Of course, these have been exploited by our intelligence community, and I understand that; but this could be an example of a distinction that is no longer meaningful.

Chair: We have got only 10 minutes left and my colleagues would like to put four questions to you, so can we deal with the questions and answers succinctly? The first is from Robin Butler, on communications data.

Q41 Lord Butler: I do not want to pursue that, Chairman, because I think Baroness O'Neill dealt with it adequately. May I ask one question that I think we ought to cover? It has been argued that some professions need special protection under the law: for example, lawyers, doctors, priests and—controversially at present—journalists. What is the panel's view about that? At the moment, the code of practice says only that "special consideration" should be given, which means that examination of such communications data is authorised at a higher level of seniority. Is that enough?

Baroness O'Neill: Special protection requires also special responsibility on the other side. A case can be made for professions in which the communication of data obtained in that way is well regulated for the medical profession—the one I know best—but also the legal profession. If one is going to make the case for journalists, I think it would have to be a completely different case.

Mr Blunkett: But it is the purpose: there is no argument whatsoever that RIPA should not be used to interfere with the normal activity of the journalistic profession—none at all.

Q42 Lord Butler: But if it was for the inquiry of a serious crime—

Mr Blunkett: Ah well, that would put it into a different definition, because that would be for a different purpose. It would be not to find out something that you could not have found in other ways, but to protect us from those dangers. That would apply whatever the profession. That was the point I was really making in *The Mail on Sunday*.

Charlie Edwards: But we have also set a precedent with, say, CCTV cameras. We have approximately 6 million, but 750,000 of them are within sensitive sites, which are in education or health. I think we have got to the stage where we understand that there are some sectors which will need some sensitivity around them, but I agree with David Blunkett that it is the act—the process of going and approaching that—that is important, rather than the law in that sense.

Chair: Menzies Campbell has a question on exchanging information with overseas partners.

Q43 Sir Menzies Campbell: Just two quick points. The first is that, of course, lawyers are not compellable witnesses against their clients under the present systems, both north and south of the border. Secondly, for the record, I regard the description "libertarian" as being something of an accolade. I have never found it impossible to reconcile my libertarianism with my responsibilities on this Committee; indeed, others currently and in the past have managed to do that as well.

On the point about exchanging information with overseas partners, we do that with the Five Eyes, as I think you all know and as is now publicly recognised, but we also do it with other countries, sometimes very substantially in our interests. Are you satisfied that the present arrangements, particularly the legal framework which exists for this exchange, are adequate, or do they need amendment?

Mr Blunkett: I am not uncomfortable with the way we operate at the moment, but it has to be on the basis of trust. You cannot legislate as to which of various agencies we will deal with, unless they are building that trust by their very nature. I was closest, obviously, to MI5 and to their relationships across the world, including in Europe. They had to be—I could not be—the judge of what information they could trust to provide to other agencies. It is quite difficult to legislate for that. Incidentally, I would like to put it on record that I have never, ever thought of Ming Campbell as a libertarian.

Chair: Thank you. If we can now move briefly to oversight questions, it is sometimes suggested that judges rather than Ministers should be the people who give authorisations. I would be particularly interested to know if any of the panel have views on that question. George Howarth, you also wanted to come in on oversight. Do you want to ask your question now?

Q44 Mr Howarth: Given the shortage of time, I will try to truncate it into one question. I think Charlie made the point that the oversight landscape is cluttered, or words to that effect. Can the panel say whether they agree with that description? Secondly, how might it be reformed in order to carry out the job of overseeing bulk interception and other forms of interception more effectively?

Professor Glees: I am not going to comment on libertarianism. What I would like to say is that in all of this, your role is absolutely crucial, and I think it is going to become even more crucial.

Q45 Mr Howarth: Sorry, can I interrupt? We are actually part of the oversight machinery.

Professor Glees: That is what I am talking about: oversight. Who signs warrants, Ministers or judges, all pales into insignificance if the public have confidence in what is being done in their name and for them. It is because I believe your Committee is the source of public confidence and accountability that I think your Committee needs great strengthening. In my paper to you, I mentioned specific ways in which I think it could be done.

At the moment, I think the public see you as being too close to the communities over which you exercise oversight. I think that if you had more staff, more research and other people—not necessarily parliamentarians—in your ranks, that would all be extremely important. The public do have memories; they know what their elected representatives may have said on this or that subject several years in the past. Basically, I think the British public deserve and want to be kept safe in a free society, and they will do what is necessary.

Q46 Chair: Can I cut you off there, because we are going to be cut off quite soon? Baroness O'Neill, you wanted to comment.

Baroness O'Neill: Very briefly, I think that authorisation and oversight are separate functions taking place at different stages of the process. I think authorisation has to be quasi-judicial for complex pieces of surveillance. I don't mean that every bit of a police investigation, for example, would need quasi-judicial authorisation—that might be done simply by rank—but authorisation needs to be, if not a million miles away, then somewhat at arm's length from operations. Authorisation is a distinct function, and it needs to be simple enough for the public to understand what the system of authorisation is.

That then comes to the oversight function. Again, we think that for public confidence that it is working, not merely this Committee but the other oversight commissioners that exist need to be well understood, and for that they need to be understandable.

Chair: Thank you. Robin, I think you have one final question on transparency.

Lord Butler: No, that has been covered, thank you.

Q47 Chair: Charlie, did you wish to make a final point?

Charlie Edwards: I have one final point. It depends on why you want to reform the current system. If it is to develop trust and confidence in the oversight arrangements, then a better informed and educated public is extremely important. Therefore, rather than necessarily more and greater transparency, in terms of greater accountability in oversight, there is a role for the ISC and others to play in communicating what they are doing and why, and why that matters to the intelligence agencies.

Chair: On behalf of the Committee, I thank all our witnesses for your very helpful and informative responses. We have the benefits of your written submissions as well and we are particularly grateful for the extra elaboration you have given us today.

11:45 AM
The session concluded