INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

PRIVACY AND SECURITY INQUIRY

PUBLIC EVIDENCE SESSION 2

UNCORRECTED TRANSCRIPT OF EVIDENCE

Evidence given by:

Emma Carr
Director, Big Brother Watch

Dr Eric Metcalfe
On behalf of JUSTICE

Isabella Sankey
Director of Policy, Liberty

Hanne Stevens
Interim Director, Rights Watch UK

Wednesday 15 October 2014
(10:00 – 11:15)

Chair: It is my pleasure to welcome you all to this session. I welcome our witnesses this morning to the second of seven public sessions during the course of this week and on other occasions in which the Intelligence and Security Committee are taking evidence for our inquiry into issues of privacy and security and matters related to that. We took evidence some time ago from the intelligence agencies; we will take evidence from the Home Secretary tomorrow; and from the Foreign Secretary and other witnesses subsequently. We are particularly grateful to you for joining us this morning, and we look forward to what we hope will be a good, lively, mutually instructive and beneficial discussion.

For the benefit of others in the room, may I invite you briefly to identify yourselves?

Emma Carr: I am Emma Carr, director of Big Brother Watch.

Dr Metcalfe: I am Eric Metcalfe, a barrister at Monckton Chambers; however, I am here today representing the human rights organisation JUSTICE.

Isabella Sankey: I am Isabella Sankey, director of policy at Liberty, the National Council for Civil Liberties.

Hanne Stevens: I am Hanne Stevens, interim director of Rights Watch UK.

Q1 Chair: Grand. Thank you. We hope this will be a relatively informal exchange. We have a range of questions to ask you. The primary purpose this morning is for us to hear your views, to contribute to our work we are doing in our inquiry. We have quite a lot of business to get through and only an hour and a quarter in which to do it, so may I encourage both my own colleagues and witnesses to be succinct in their questions and answers?

We have seen the written submissions you have helpfully sent us. Would any of you be prepared to give us an initial comment on the general question of privacy and security and the relationship between the two? We have suggested that there needs to be a balance; some have questioned whether balance is the right word.

Isabella Sankey: "Balance" can be unhelpful sometimes in this debate, because it implies that the two are always working in opposition to one another. We believe that privacy is essential for security, and vice versa, and the human rights framework provides that both must be protected, so the idea of pitching the two concepts as a dichotomy is unhelpful. It also leaves out of the debate many other rights and protections for which Government are responsible—privacy is essential for liberty, for freedom of conscience and for many other human rights values to which our nation has subscribed for so long. It narrows things and unhelpfully sets the two in opposition.

Q2 Chair: That is very helpful. May I question you further on that? Is there any question of an absolute right to privacy, or is it accepted that there are legitimate occasions on which the state or the Government, or whomsoever it might be, is entitled, and it is right and proper, to reduce some elements of privacy in the interests of the safety of the public, or for other reasons of that kind?

Isabella Sankey: Absolutely. The right to privacy is a qualified right and it can be interfered with for a range of purposes, including for the protection of the rights of others. Similarly and interestingly, the right to life is not an absolute right. The state is permitted to take life in exceptional circumstances. So describing either as absolute is misconceived as well.

Q3 Sir Menzies Campbell: I understand the intellectual criticism of the word "balance" but these are two characteristics which have a relationship with each other. It seems to me, and I would be grateful to know whether you accept this, that in a time of relative peace the balance—forgive me for using the word—between privacy and security might well tend towards privacy. In a time of relative danger, when the interests of the country and the safety of the citizens are at stake, the emphasis may be on security. How should we determine where the emphasis needs to be put at any particular point? In the end this is the responsibility of Government. Is it enough that the Government should have to make these decisions?

Dr Metcalfe: With respect—

Sir Menzies Campbell: That is always a very dangerous beginning.

Dr Metcalfe: I would say that it is unhelpful to deal with questions such as privacy versus security in general in abstract terms and to suppose that a balance can be struck in general terms for the sake of a general situation. I think you always have to look at the specifics. You have to look at the context. You have to look at the particular measure that is being proposed and ask, "How is it justified not only by the particular circumstances such as a threat—a specific threat—or a more general threat of post-9/11 security concerns?" You also have to ask: "What is the aim that you are pursuing?"—it is generally national security and the prevention of serious crime—and, "Is that aim necessary? Is the restriction that you are proposing proportionate?" That is a much more particularised question. I agree with everything that Bella has said. But to talk in general terms about being under threat now, so we need more security and less privacy, does not really assist.

On a more general point just to add on to something that Bella said, it is important to bear in mind that the right to privacy is not just an individual right but a public good. It exists not only for my own benefit but for all our benefits. Society as a whole is better when each of us have our right to privacy respected. That is true not just when times are good but also when times are tough. I would go so far as to say that it is especially true when times are tough. It is even more important in times of crisis and times of threat that we remember what our fundamental rights are.

Sir Menzies Campbell: You use the word "context", which I thought was very interesting. We don't have the threat level up on the annunciator screen at the moment, but if it is enhanced does that make a difference?

Emma Carr: What we are defining as national security and threat is extremely broad. I think if you asked any member of the public whether they supported intelligence agencies or law enforcement having the tools to tackle national security they would agree. I think national security as a definition has become extremely broad, and we have seen that with the development of RIPA since 2000. I think we all agree that it was initially brought in to tackle elements of national security, but now, when we have applied for information through freedom of information or when we have requested information on why certain tools like RIPA are being used, it is defined in the terms of national security, and I think that when they were first defined it certainly would not have been there.

Q4 Mr Howarth: Would it be helpful if we could look at a specific case—a known case—and work out at what point there is a concern about it? I am talking about the case of Roshonara Choudhry, who stabbed Stephen Timms at a surgery. Her radicalisation took place entirely online, and it started off with looking at various sermons that gave a particular Salafist view of Islam. That, presumably, is okay and off limits. The second phase of it was to get in touch with organisations online that were promoting jihadist activity. Again, that might be acceptable. Finally, she got linked into the online magazine "Inspire", which gives specific instruction in how to construct a bomb. At what point in that spectrum do you think the state has a legitimate interest in intervening?

Isabella Sankey: When an individual gives cause for suspicion that they are planning some criminal activity, whether it is terrorism or other forms of crime, Liberty does not take issue if they are then subjected to targeted surveillance. But the reason why I think this inquiry has been convened in response to the disclosures that we had last year is not because the state is engaged in only looking at the communications of individuals who are considered to pose a threat, but because it is currently engaged in looking at millions more communications.

So, on the issue of targeted surveillance, we are getting into specifics. If somebody gives cause for concern, fine. But RIPA, as Emma has already mentioned, does not require reasonable suspicion or any link to criminality before its powers can be exercised. It contains huge numbers of loopholes, which we now understand has allowed our security services to surveil, to intercept and to require data communications data on a scale never previously imagined, and this has come about in the last couple of years without public or, we understand, significant parliamentary understanding or approval.

Chair: Your answer has taken us into what was going to be our next area of questioning on the area of targeted intrusion. Julian, we can probably be brief.

Q5 Dr Lewis: You have taken this forward extremely well. I assure you that you have our solemn promise we will get into this whole question of bulk monitoring, but, in order to nail things down, is there anybody on the panel who disagrees with the proposition that where there is specific intelligence that an individual poses a direct threat to the United Kingdom, it is proportionate and appropriate for the agencies to investigate that individual and for that investigation to intrude on the person's privacy? You have already given your answer, Isabella. Does anyone disagree with the answer we have already had from Isabella?

Dr Metcalfe: In fairness to Ms Sankey, the way in which you phrased the question—I am sorry for being legalistic, but this is my daily bread and butter—can give rise to some slippage. The specific test is whether specific powers can be used in relation to that individual. You have referred to direct intelligence that the person is a threat, but you would of course have to assess the quality of the intelligence, because intelligence can be extremely high quality or extremely low quality. Merely to have some intelligence that a person was a direct threat would not itself justify the use of intrusive powers.

Q6 Dr Lewis: I am afraid that the terminology I used was "specific intelligence", and I think that that is a clear enough suggestion. Obviously, you have to make judgments in each and every case, but we will not get very far if we get to that level of nit-picking. In reality, the position you seem to be taking—unless anyone disagrees—is that, where there are grounds for reasonable suspicion that someone ought to be investigated, it is appropriate for that person's privacy to be compromised by an investigation. Is that right or wrong?

Dr Metcalfe: I would agree that it can be the trigger for more intrusive powers to be used.

Q7 Dr Lewis: I will take that as a yes but, as we have limited time, it would be appreciated if you were a little more direct.

Hanne Stevens: In the example you used about Choudhry, that would inevitably throw up the surveillance, monitoring, analysis of telephone evidence and the names of colleagues, associates and friends of that person who were entirely innocent. There is also responsibility to act appropriately in relation to superfluous or irrelevant data. It is important to remember accountability and oversight, and I am sure we will come to that in due course.

Q8 Mark Field: We are obviously living in a fast-changing world because of technological advances over the last decade or so, and who knows the pace at which that will continue. We all appreciate that that must have a bearing on ensuring we have workable legislation. In the last 14 years since RIPA, we arguably now have what is, to a large extent, fairly defunct legislation. Do you think that monitoring an individual's internet communications is more intrusive than the more traditional types of surveillance from a bygone era, such as opening people's mail or tapping their telephones? If so, why? Why should we keep a closer eye on that today than we would have a few decades ago?

Dr Metcalfe: I do not know that it has to be more intrusive; it simply has to be as intrusive. It is as intrusive as opening your mail or listening to your telephone conversations. You should take it more seriously now to an extent because we spend far more of our lives online now than we did even 14 years ago. Some people were online quite a lot 14 years ago, but most were not. Most of our transactions are now handled online. Most of our private relationships are conducted in some way via the internet or fibre-optic cables each day. The infrastructure of the internet is basically carrying and, in the course of doing so, recording every aspect of our daily lives.

Q9 Mark Field: Is there not an issue of implied consent? With quite a lot of what we do online—for example, buying products online—we kind of know that our past record of sales and purchases will be picked up and fed through. There is more of an implied consent in people using the internet on a day-to-day basis than there was with some techniques in the past.

Dr Metcalfe: With respect, my consent is entirely one-to-one—if I buy a book from Amazon, I expect Amazon to be bound by its duties under the Data Protection Act to secure my data, just as I expect Royal Mail not to open my letter and tell people what I am up to. The same absolutely goes for Amazon, and there is no more implied consent in me ordering a book online from Amazon than

there was 30 years ago if I ordered a book through the post from my local bookshop. I have the same right to the integrity of my communications.

Isabella Sankey: Just because you choose to do something online, it does not mean that your expectation of privacy should diminish. Just because you go into a bookshop to buy a book, you do not implicitly consent to someone sent from GCHQ to be standing by the till making a note of the fact that you have bought that book.

Q10 Mark Field: Someone from Waterstones might well send you details of similar books in a few months' time because of the book you bought.

Emma Carr: The important point here is about the rate and ease of analysis. With internet communications, it is very easy to look for a name or specific information and then look for everything that corresponds with that and analyse it. Post, CCTV footage and things like that are a lot harder to analyse. That is where I think the difference in intrusion comes in.

Dr Metcalfe: To clarify, I would concede that there are parts of the internet that are entirely public, and it is legitimate for that material to be expected. If I broadcast my opinions to the world on Twitter, I can hardly complain if someone takes note of those opinions and later uses that information against me. But you have to be very careful and always look at the particular case. Just because I put a post on a friend's Facebook page, it does not mean that I have lost the expectation of privacy.

Isabella Sankey: Similarly, the expectation of privacy does not mean that the internet should be an unpoliced place. As Eric says, there are public spaces on the internet, but even in those private spaces, where you are talking about e-mails and messages sent over the internet, the expectation of privacy should absolutely remain. That does not mean that, in the circumstances we have just heard described, that cannot be compromised when somebody exhibits suspicious activity.

Emma Carr: That is the very specific thing. Any decent member of the public would expect that if you write something online and are suspected of a crime, there are ways and means of law enforcement to access those communications. Everybody understands that. If you are not suspected of anything, that is where the line comes in of having the right to privacy online; that is whether online or offline.

Q11 Lord Butler: Are you concerned about non-state intrusions of privacy as well as state intrusions?

Emma Carr: Yes.

Isabella Sankey: Yes, absolutely. There is a difference between state and non-state actors in principle, because state actors have very coercive powers over individuals: the ability to prosecute, put on trial, in our country to take away somebody's liberty and in other countries to put them to death or similar punishments. So there are distinctions in principle, but it seems the lines have become so blurred between the activities of non-state actors and state actors that the concerns that we have about state actors certainly apply equally to non-state actors.

Dr Metcalfe: That goes back to a point I made earlier about my rights vis-à-vis Amazon, for example. It is interesting that now, in 2014, much of the regulation of what we might consider traditional surveillance—gathering information about people for whatever purpose, including the detection of crime—is governed in large part by data protection as much as RIPA. The data protection framework is now a large way in which we regulate the way in which data can be collected, retained, used and so on.

Hanne Stevens: The state is under a different duty, to protect not just our national security but our privacy. Non-state actors such as private companies are not under the same duties. Arguably we have higher expectations of the state in relation to our individual rights.

Q12 Chair: I now want to come on to whether there are particular people who deserve special protection. We would all agree that intrusion must be proportionate. In other words, it is more justified if the suspicion is of a more serious crime. But are there categories of people who deserve a higher bar to be set? I am thinking of lawyers, religious figures, doctors or journalists. Do you think any distinction needs to be made on that spectrum of the type of people who might be targets of intrusion?

Dr Metcalfe: Again, I think it is more important to look at the function rather than the category. I do not have greater right to privacy because I am a barrister than someone who is not a barrister. I do, however, in relation to the specific work that I do—my day-to-day functions as a barrister when I am giving legal advice and so on—have greater protection. That is not only for my benefit; it is more for my client's benefit. It is also for the court's and the public's benefit, because we recognise the importance of people having the right to receive confidential legal advice on their affairs.

Emma Carr: It is very important, but it is also somewhat arbitrary. A lot of the time when you see potential misuse of these surveillance powers it is because they are being overused and not overseen properly. There is a lack of accountability and transparency in how they are being used. That has been very much put in the public domain with the police use of RIPA and journalists' records. I think that is due to a lack of understanding from police forces themselves of how RIPA is supposed to be overseen and the authorisation process, and the public knowledge about how easy it is for police to access communications data.

Q13 Sir Menzies Campbell: Back to the question of state and non-state actors. Did I understood you correctly? If my purchasing pattern becomes known to Tesco, does that deserve the same protection as, for example, my blood group or the people I associate with? If so, how do we enforce that, not least because there appears to be some trade in that kind of information?

Dr Metcalfe: You enforce it through the data protection framework. That framework stops Tesco in principle selling that information to a third party without your consent. One difficulty in the modern day and age is that we all sign up to various services and do not look closely at the fine print. We do not realise. When we are asked whether we accept the terms and conditions we most often tick the box. One of the conditions will be that Tesco, or whoever else, may use this information and may sell it on to third parties for the use of various services.

Isabella Sankey: But ultimately companies are creatures of statute that can be regulated by states and Parliaments. Just as, in our view, the security services have over-reached when it comes to their privacy infringements, so, too, it may be the case that private companies have and regulation has not kept up.

Dr Metcalfe: To address the specific point, my purchasing history is private information about me in the same way as my medical information. In fact, you can probably tell quite a lot about my medical status or what I do in my private life from looking at my credit card record.

Emma Carr: It is how you link up all of that information. Your loyalty card data from a supermarket might in itself be useful only to that supermarket, but if that is linked up with your medical records—which I think at one point was a policy suggestion—to see whether you are buying four pizzas a week, and your gym membership data to see how often you are going to the gym, you get a more accurate picture. Those things in themselves are not particularly intrusive, but if we build that bigger picture, which is there and available, they become far more intrusive.

Chair: That has been a very helpful discussion, but it is now time to move to one of the core issues that we would like to hear to views on. I think there has been broad agreement that, when people are a threat to the safety of other citizens, it is right for the agencies to be able to take action to find out what they are up to. So we come to the question of how they can do that. Part of the debate is: should they have access to what is often referred to as "bulk interception" in order to identify who might be a threat to the public safety? Lord Lothian will ask a question.

Lord Lothian: You asked my question just now.

Chair: I did not intend to. Do you want to expand on the question?

Q14 Lord Lothian: This is really just beginning to open the debate on bulk collection. Certain categories of threats to our society—terrorists, criminals—go to great lengths to conceal their identities and what they are doing. Therefore, it is presumably acceptable that the state has the means to try to find out who those people are. To do that, obviously they have to go beyond the targeted technique that we have been talking about. Do you accept that the state has the right to collect communications to try to establish the fact, which until then is unknown, of who intends to do what that could be a danger to our society?

Hanne Stevens: Mass and indiscriminate surveillance does threaten citizens' fundamental rights, and these rights cannot be circumvented or traded off against any perceived benefit unless that is in full compliance with an adequate legal framework. We are not currently enjoying that position, with RIPA being so outdated and the categories being—

Q15 Lord Lothian: We will come on to the framework later on. I am trying to establish whether you accept that, for instance, in order to find out what terrorists are plotting, you may have to go beyond targeted techniques and be able to collect information.

Dr Metcalfe: Again, the problem is the way in which you talk about collection. You move from "Targeting doesn't work, so we need collection beyond targeting" to address that problem. But let me put it this way—

Q16 Lord Lothian: I am not saying that targeting does not work; I am saying that, in order to get to targeting, you may have to collect information to decide who you are going to target. I am asking if you accept that.

Dr Metcalfe: Then allow me to address it that way. My point is that your collection would also have to be targeted. You cannot simply say that because the targeted approach under section 8(1) of RIPA, which covers particular persons or premises, does not work because you cannot identify the particular person that you are looking for, ergo, bulk collection on an indiscriminate basis is justified. That is a false premise. In that situation, if you are trying to identify a person unknown—a John Doe, as it were—who is involved in very serious terrorist activity, then the collection of data of communications unknown also has to be targeted.

Say you know that the person unknown visits this particular site at this particular time, even though you do not know other things about them. It would be reasonable and proportionate in that circumstance to collect communications of a particular group or category of individuals visiting that site at a particular time of day, so long as that group was not so large. If, for example, five people a day visited this particular website, it might be proportionate in those circumstances to collect the information of five people. What has been disclosed from the Snowden revelations and so forth, on the other hand, is an different category. If the reports of Tempora are true—and you are in a far better position to know than any member of the public—we are seeing a 13-day rolling buffer of all communications going across fibre-optic cables and all communications data being retained, for which there is no safeguard under section 16 of RIPA. That is profoundly concerning. In crude terms, it is the largest breach of privacy in British history.

Emma Carr: With all of these things, over the past decade, every policy solution has been to collect more data. That is usually because there is a feeling that traditional methods have failed. From my perspective, it is because traditional methods have failed to keep up with either the rate of investigation or the rate of technology. You just need to look at recent examples. The NSPCC released an FOI last week showing that hundreds and hundreds of pieces of hardware are sitting in

police forces, because they did not have enough digital forensic experts to go through and look at them. Clearly, that is not acceptable.

The Julian Huppert case was raised in the Commons yesterday, to which the Home Secretary responded, where CEOP had failed to react to 2,500 names of potential paedophiles. Again, that is not an acceptable place to be. It is because of a lack of technical ability and awareness within traditional police forces. It was not because they did not have the data in any of those cases, it was because they did not have enough capability to go with it. That is a huge problem that we need to face, and we have not done that yet.

Q17 Hazel Blears: I want to follow up some of the points that witnesses have made about "indiscriminate surveillance"—I think that was the phrase used—which is a major concern. Obviously, the analogy has been drawn that, if you want to develop targets, and you do not have information about specific individuals, you have to have the pool of information in order to be able to target it. I do not know whether you have an objection in principle to the collection of bulk data or whether your objection is to the interrogation of that bulk data. If you simply object to the collection in principle, you would be limiting the possibility of the agencies in developing targets for future examination.

I am quite keen to get your view on whether you object to bulk collection, per se, or whether your concern is about bulk interrogation of that data. If you are going to interrogate the data, you have to do it with a targeted search, you have selectors, you have filters, so there are ways in which that bulk collection can be subject to targeted interrogation, which is covered by a legal framework. I do not know whether you object to the bulk collection, or whether you object to the interrogation of that collection without proper safeguards.

Isabella Sankey: The objection is to both—the collection and the interrogation without an appropriate framework. There is nothing passive about GCHQ collecting millions and millions of communications of people in this country, indeed having the power to collect all communications outside this country, because it falls within the external communications definition, even if human beings are not processing those communications and it is being done by machines. That is a physical interception—a privacy infringement—and a model of blanket interception that we have not traditionally followed in this country .

Q18 Hazel Blears: I understand that, and I think it is important that we get this on the record—that your objection is to the bulk collection in the first place. But would you accept that, in order to develop targets—people that we do not know yet and do not have reasonable suspicion about—how are you going to gain that information unless you have the pool of information in the first place that can then be subject to interrogation?

Dr Metcalfe: The concept of the pool here is the way in which the concept of bulk slips in, because the supposition seems to be that as soon as you are unable to identify a particular individual, you can throw the net as wide as you like, which cannot be true. The idea that collection itself is not an interference is, again, with respect, absurd. Imagine if you took my diary and said, "Don't worry, we're not going to read this unless we get a warrant from the Home Secretary." Or you could easily turn around and say, "Let's put a CCTV camera into everyone's bedroom in the country, but we won't be able to turn it on until we have an authorisation from a judge." The very act of collection is itself the intrusion on privacy in many ways, whether or not it is ever looked at. We can look at the situation in 2008, when Liberty won its case before the European Court of Human Rights. Collecting the DNA—the intimate genetic information—of individuals who had not been charged or convicted of any criminal offence was held to be a fundamental breach of their right to privacy. The same is true if you take my letters, my diary or footage of my house: even if you never look at it, there is an interference in my privacy. Part of it comes from the uncertainty; I can't ever know for certain, whether you have looked at something or not.

Q19 Hazel Blears: That brings us back to—I won't call it a balance, because I don't think that is the right definition—the fact that you have a right to privacy, which is subject to constraints through legal authorisation. But you are saying that bulk collection is a step too far in terms of infringement of privacy and, therefore, that if we are unable to analyse targets and develop targets in a way that, subsequently, would contribute to national security, you are prepared to forgo this possibility because of the intrusion into people's privacy. Your balance falls in not having bulk collection at all.

Isabella Sankey: Absolutely. There are many ways in which the security agencies have abilities and powers to trace suspicious activity without having the bulk of information on the scale that we have seen. We understand that this is something that has only come about over the last few years, and it was a policy change immediately after 9/11 that led to the idea of this bulk collection. The reviews that have been conducted to try to investigate whether bulk collection has reaped the security benefits that the agencies claim have all concluded that that analysis is, indeed, flawed. The Obama White House-appointed review group found that the NSA's programme of bulk interception and metadata acquisition was not essential to preventing attacks and that information needed to disrupt terrorist plots could readily have been obtained in a timely manner using conventional court orders and traditional investigative measures.

Q20 Hazel Blears: If there were evidence that the ability to have bulk collection and then to interrogate it through targeted searches that are properly authorised under a legal framework had helped to develop targets, prevent plots and contribute to national security, would your view be different?

Dr Metcalfe: No.

Isabella Sankey: No. Because that comes down to what kind of society you want to live in. Do you want to live in a society where a framework and an institutional capability has been set up which fundamentally alters the relationship between the individual and the state in a way that we have never considered doing in Britain, or do you want to live in a society where there is proportionate surveillance?

Hazel Blears: I understand that, and I am grateful for your clarity on that issue.

Q21 Dr Lewis: Yes, it has been clear. I just want to put one point to you. The people who defend the pool are categoric in their denials that they do not go fishing at random—that they do specific searches. I want to come back to the helpful example you gave, Dr Metcalfe, when you said that if someone knew that somebody they wished to identify had visited a certain website, and providing that there was not a mass of visitors to it, it would be okay to do a targeted search of who had visited it, to narrow down the list of suspects. Without getting too tied up in the individual specifics of that example, that seems to suggest that you must have some sort of pool, or mass basis, of data as to who is visiting websites, for example, to make that targeted search. How do you reconcile that example, which you yourself gave, of a justified search, with your very clear collective view that there is no justification for having the pool in the first place?

Dr Metcalfe: Let me point to RIPA itself. Section 8(1) allows you to target communications of a particular person or a particular premises. Very often, you are not going to know that a particular person is involved in, say, serious organised crime, drug trafficking or whatever, so you are going to start with a suspicion that a particular location is being used—

Q22 Dr Lewis: Can't we stick to the example of the website, which was rather more relevant?

Dr Metcalfe: No, because I think the premise of this example actually illustrates what I am talking about. You do not know the identity of the people involved, and there may be—in fact, there

are entirely likely to be—innocent people who are collaterally caught up in your interception of communication at the premises. RIPA already allows for the collateral interference with people's privacy, because you have suspicion against a particular location being used, though not the particular individual. Targeting the premises will allow you to identify the individual. Once you have targeted the individuals concerned, you will be able to—

Q23 Dr Lewis: With respect, that is taking it right away from the helpful example you gave before, because this business about bulk collection is mainly about bulk collection of data online and so forth. You gave an example where it would be justified in your view to home in on a particular website and all the people who had visited it. And yet, if you do not have the bulk data collected, you cannot possibly do that, or at least you cannot do it retrospectively, can you?

Dr Metcalfe: Why can't you get a targeted warrant in respect of the particular website that—

Q24 Dr Lewis: Okay, so in that case you would only be able to look at it in the future; you would not have any ability to go back to see who had been visiting it.

Dr Metcalfe: With respect—

Dr Lewis: I don't need respect, I need the answer.

Dr Metcalfe: It would be very nice for all investigators to have a time machine, but the idea that you should collect private information about individuals at a point when you have no suspicion that they are involved in any crime—

Q25 Dr Lewis: In other words, you can only go forward; you do not have the ability to go back and see who visited that website in the past. Is that what you are saying?

Isabella Sankey: In the same way that you cannot bug a person's car retrospectively, you cannot intercept their conversation retrospectively.

Dr Metcalfe: It is also false to say that you cannot. Once you have established suspicion, if you have available records, you can under certain circumstances make a request under chapter II of part 1 for the communications data in respect of that. I think you are leading to a more general question, which was addressed by the Court of Justice to the European Union at Digital Rights Ireland in April this year. You cannot justify retaining the communications data of the entire population of the European Union for a period of up to two years, simply because of the suspicion that some of them might commit crime and be involved in terrorism and that therefore it will be valuable to go back.

Q26 Dr Lewis: But your view is that if you are going to target an online database, it basically starts from the moment you have identified it. You have to go without the potential resource of seeing who has visited it in the past, unless there is some other record that can be accessed by specific application.

Dr Metcalfe: You have to have the suspicion before you can get the target. The target cannot precede the suspicion.

Q27 Mark Field: You have been very candid about this whole policy, and I would probably share some of your scepticism about the security services saying, "We desperately need all of this, and that the way in which we have thwarted attacks since 7/7 has been because of these powers." Is there a concern that, if we had the ideal world that we have discussed, where we were not allowed bulk data, we would return to some more traditional means that might end up being considerably more intrusive, particularly with a heightened terror threat, which might undermine some of the planks of the sort of society that all of us want to live in? If we start having some more old-fashioned surveillance techniques being used, particularly on parts of the UK community, in a much more

aggressive way, that may undermine what you are doing. With bulk collection, much of those data are never used, and there is neither the capability nor even the capacity to be able to deal with anything other than a small proportion of that, which will only come to light when particular individuals are suspected of terror activity, paedophilia or other crimes.

The worry is that if we step back from this and draw a line, and say that we are going to do nothing whatever in the internet age and go back to old techniques, we will have a very different, much more intrusive society going forward.

Dr Metcalfe: The intelligence services and the police have incredibly powerful and intrusive techniques right now, which are entirely legitimate. We are talking about going a step beyond targeting to bulk collection. I do not accept that we have to allow for bulk collection because the alternative may be even worse. The alternative always has to be measured by reference to protection of fundamental rights. If the alternative is equally bad, then it is equally bad. It is not a justification for bulk collection.

Q28 Chair: Before we move on from this subject, can I ask you to clarify what I think has been perhaps one of the most important pieces of evidence that you have given us? You expressed your belief that bulk interception does not, in practice, produce any substantial benefits. I accept that is what you believe on the basis of what you have expressed. However, you were asked whether you would still be opposed to bulk interception if there was hard evidence that it had produced significant material that led to terrorists being apprehended or prevented from carrying out their deeds. I want you to clarify because, as far as I am aware, each of you said that even if that could be demonstrated, you believed that on the proportionality argument, it was still unacceptable for the intelligence agencies to have access to bulk interception. We have understood that to be your position. I want to be clear; this is an opportunity to say, "Yes, it is" or to qualify it in an appropriate way.

Emma Carr: As far as I am concerned, there has been nothing shown in the UK to show that. For millions—

Chair: That is not the question. If evidence did emerge—

Emma Carr: You are asking us about if we were asked to believe some evidence that had been presented to us, but every time that we have been asked to do that, it has been shown to be incorrect, or not as effective as—

Chair: Hold on; let me ask the question, and then please try to answer it. It is quite simple. We are not asking you to accept that there might be occasions when this did happen. I am asking you a question of principle. As a matter of principle—

Isabella Sankey: As a matter of principle—

Chair: Let me finish my question, please. Then you will have an opportunity to answer. If evidence emerged through bulk interception that even you acknowledged had led to terrorists being arrested or prevented from carrying out their objectives, are you saying that, as a matter of principle, you believe so strongly that bulk interception is unacceptable in a free society that you would say that that was a price we should be willing to pay, rather than allowing intelligence agencies to use bulk interception methods?

Isabella Sankey: Yes.

Dr Metcalfe: Yes. Just as you would solve a lot more crimes if you had CCTV in everyone's houses, and if you opened everyone's mail and e-mail and read it on a daily basis. Yes, you would solve a lot more crimes and a lot more terrorists would be in jail; that would be a good thing, but it would be bad for our society as a whole.

Q29 Chair: And that is the view of your colleagues as well?

Emma Carr: Yes.

Q30 Lord Butler: If you have bulk interception, and indicators throw up 0.001% of things as suspicious, why does that not satisfy your definition of a targeted search?

Isabella Sankey: Because you have already intercepted people's correspondence. The analogy is that in the 1980s or 1990s, we suddenly decided to start taking copies of everybody's mail that was travelling through Royal Mail, in case in the future we could run some new, advanced technology on it and work out if there was any suspicious activity that we wanted to follow up. If you take a traditional example of communication like that, people would know that it was unacceptable. Just because it is easier and cheaper to do that because of the digital revolution does not mean that it is okay to do, or that it is what we should be doing.

Q31 Lord Butler: Despite the fact that it has not been looked at by any human actor?

Isabella Sankey: Absolutely, because you have built the physical infrastructure to allow probably the worst type of oppression in the future. In any free society, it is not just about saying, "Take it on trust: we're not going to use it in this way. We're just letting the machines do it." It is about examining what physical infrastructure you are building, the relationship between the individual and the state, and not just expecting to take it on trust and to accept the fact that not much of the material is currently looked at.

Emma Carr: It is the threat—

Q32 Mr Howarth: There is an argument that because the collection of bulk data is, I think you have all agreed, in principle wrong, there should not be any collection of bulk data. It is difficult to prove, but let us just say theoretically that, in neglecting to do so, an horrific terrorist activity took place. The argument goes that the intervention in privacy is so great that it is worth taking the risk, and even bearing a small number of incidents, rather than breaching the principle. Would you agree with that argument?

Dr Metcalfe: You can always build hypotheticals to justify any breach of fundamental rights, no matter how much of a breach. You can always say, "Yes, the right to liberty is really important, but if it would save a million lives tomorrow would we do away with it today?"

Q33 Mr Howarth: But this isn't hypothetical. This is about something that is already going on. It is about data that exist and whether they may be exploited. You object to that in principle, which is fair enough, but do you accept the corollary to that, which is that some things might happen that otherwise might have been prevented?

Isabella Sankey: Yes. That is always the case in a free society. Some things might happen that could have been prevented if you took all the most oppressive, restrictive and privacy-infringing measures. That is the price you pay to live in a free society.

One of the problems with answering these sort of hypothetical questions, put that way, is that all the current resource that has been going into bulk collection—the manpower and the money spent on that—is necessarily money not being spent on other forms of investigation. It is almost impossible to answer the point, "But for this bulk collection, we would not have been led to x suspect or y suspects," because all the time you are dealing with a hypothetical and with resource that has not been used in another area.

Hanne Stevens: In relation to bulk data we should try to dwell on what is actually going on, rather than the various different scenarios. In fact, it is being collected and it is not being well regulated. That is a concern. There must be more scrutiny of that and more resources put into the oversight of those who are doing the surveillance. There is some merit, obviously, in dwelling on the rights and wrongs of bulk data, but let us get back to the reality. The fact is that it is happening and needs far better regulation.

Q34 Chair: If we have the time, that is one we will want to cover as well. You have been very frank in your answers, and we are grateful to you for that. Can we move now to the question of the actual legislation that exists and whether there is a need to reconsider whether it is appropriate? RIPA has been described as an analogue law in a digital age. Each of your organisations has indicated a need to reform RIPA. Could you give us some examples of the kind of changes to the legislation that you yourselves would recommend—not just whether it should be reformed, but the kind of changes that you would recommend that we should endorse?

Dr Metcalfe: The first important safeguard is judicial authorisation for all intrusive surveillance under RIPA. At the moment you have a patchwork system, where different bodies are responsible for authorising different kinds of surveillance—some internally, some by a Secretary of State and some by a judge. It is a highly unsatisfactory framework. Interception—on a traditional view, the most intrusive form of communications surveillance—is authorised by a Secretary of State. If, however, the police want to plant a listening device in my house or my car, they get authorisation from a surveillance commissioner, who is a retired judge. Then, if someone wants to access my communications data under chapter II of part I of RIPA—let us say it is the Metropolitan police—they do not go to a judge or to the Secretary of State; they go to a senior designated person within their organisation and get authorisation from them.

Q35 Chair: The principle behind that, rightly or wrongly, has been that the greater the degree of invasion of privacy, the higher the level of authorisation that should be required. Do you not accept that as at least a reasonable principle, even if the way it is being applied might not be satisfactory?

Dr Metcalfe: I see the principle, although—again, with respect—I would query whether a Secretary of State is a higher form of authorisation than a judge. A judge is independent and impartial. A Secretary of State, however diligent and conscientious, always represents the views of his or her Department and is accountable in Parliament.

Q36 Fiona Mactaggart: If the Secretary of State was allowed to report to Parliament on this issue, would that change your view of this, Parliament being accountable to the people? Of course, a judge is not accountable in that way.

Dr Metcalfe: It would be very interesting to see a politician be accountable for his or her surveillance decisions. I suspect that it is not appropriate, in exactly the same way that search warrants authorised by Secretaries of State have not been thought appropriate in this country for some 400 years. We would consider it intolerable—indeed, 400 years ago it was thought intolerable—for the Secretary of State, or the Home Secretary of his day, to be able to authorise general warrants in respect of people's correspondence. That was struck down by our courts, and for 400 years it has been settled law in our country. There is something extraordinary about a situation in which a Secretary of State can authorise intrusion into my private communications and my phone calls, but a judge is needed to get a search warrant for a person's house. It seems to me that the judge should be in the same position, although I agree that there is an argument to be had about the type of judge.

Q37 Chair: Is your argument one of principle, or are you suggesting that the Secretary of State does not apply the same amount of time and detailed consideration to it?

Dr Metcalfe: It is not the time or consideration—I am fully willing to allow that the Secretary of State devotes a lot of time to it—or that they are slapdash or rubber-stamping, but simply that they are institutionally ill-placed to balance the fundamental rights of the public interest and the rights of the individual, which are also in the public interest, in that kind of situation. To give you a brief

example, after 9/11, the Home Secretary—you heard from a former Home Secretary, David Blunkett, yesterday—was undoubtedly under tremendous pressure to prevent attacks in the United Kingdom. The Home Secretary is accountable to the public for their protection. It is easy for a politician in that situation to say, "Well, yes, this is going to interfere with the privacy rights of innocent people, but I think I will be judged at the ballot box more by the number of people I have saved."

Q38 Chair: Has not the FISA court in the United States, for example, been subject to exactly the same criticism?

Dr Metcalfe: That is a judgment made by a judge. I can address the FISA court in more detail, but it has a slightly different context. The point is that an independent judge might come to exactly the same decision, but the quality and nature of the decision are different because the judge is independent of political pressure.

Q39 Dr Lewis: I want to give you the opportunity to give your assessment of the adequacy or otherwise of the European convention on human rights and the UK Human Rights Act in relation to interception. The interception of the content of communications is permitted only if it is lawful, necessary and proportionate. Having a lawful purpose means that it has to safeguard national security, including economic well-being and the prevention of serious crime. First, do you think those are legitimate reasons for allowing interception under those Acts? Secondly, necessity is taken to mean that the information that is being sought cannot be obtained by less intrusive means. Do you consider the doctrine of necessity a valid safeguard, or would you like to see changes to strengthen it? Finally, proportionality means that it must be no more intrusive than is justified by the purposes of the investigation and must consider the impact on the privacy of innocent people, which we have discussed a lot today. Do you consider that the proportionality provision is a sufficient safeguard? Please give your response and an overall assessment of that provision.

Emma Carr: I am not a human rights lawyer by any stretch. An interesting report came out of the UN today by the special rapporteur on counter-terrorism. It states, "merely to assert—without particularisation—that mass surveillance technology can contribute to the suppression and prosecution of acts of terrorism does not provide an adequate human rights law justification for its use…There is an urgent need for states to revise national laws regulating modern forms of surveillance to ensure that these practices are consistent with international human rights law." That pretty much highlights what Big Brother Watch is thinking on this issue, without its being a human rights organisation.

Isabella Sankey: As a statement of principle and an overriding framework, I think article 8 of the European convention, as incorporated by the Human Rights Act, does a good job of setting out the considerations for when and how interception should be allowed. The problem is that our more specific piece of legislation, RIPA, does not incorporate in its spirit, although it may in its letter, the principles that have been elaborated by the Strasbourg court in incorporating the convention. The fact that under sections 8 and 20 of RIPA, external communications—those completely outside the UK, or where one point is coming from or to the UK—can be authorised in bulk means that you are already driving a coach and horses through the principles of necessity and proportionality. That is where the current problems with RIPA lie. Although it incorporates the words "necessity and proportionality", the specifics of how interception can be authorised do not adequately protect those principles.

Q40 Lord Lothian: In a sense, leading on from what you have just said, the difference between RIPA 8(1) and RIPA 8(4) is that RIPA 8(4) deals with external communications and the

threshold is lower. I just wonder whether in general you have any comments on the differences between 8(1) and 8(4) in that regard. Do you think that the thresholds should be the same?

Dr Metcalfe: It is extremely problematic. It is basically contrary to the very principle of proportionality, because how can bulk collection of communications data ever be proportionate, if it is not targeted? Targeting and proportionality go hand in hand. The main problem, however, with section 8(4) is not only that it is in principle untargeted. The definition of "external communication" under section 20 is extremely vague. It has become even more vague in the light of the witness statement of Charles Farr earlier this year in the proceedings before the Investigatory Powers Tribunal, in which he indicated that a Facebook post on a friend's Facebook page is considered to be an external communication, so if I post on a friend's Facebook page and I know that that person has two other friends, both of whom are my friends, that is considered an external post because it is going to a server in northern California owned by Facebook, whereas if I send that friend an e-mail, that e-mail, even though it may be routed outside the United Kingdom, will be considered an internal communication so long as my friend is within the United Kingdom. It leads to absurd results.

Q41 Lord Lothian: What would be your reactions if, rather than just a blanket net being cast in terms of looking at these communications under RIPA, you were looking under categories of communications? I shall give you two examples relating to potential terrorism. We know that Yemen is one area that terrorism can spring from. We know at the moment that Iraq and Syria are also, with ISIL operating there, areas that terrorism could spring from and have an effect in this country. If communications arising out of those areas were targeted, would that make it more acceptable to you?

Dr Metcalfe: It is a narrower form than intercepting everyone's communications, but of course, under section 5(6) of RIPA, there is the additional allowance that you are allowed to intercept any communications, whether internal or external, as are necessary in order to obtain the information you are looking for. Perhaps you are looking only for one particular set of communications between someone in ISIS and someone in London, for the sake of argument, but the technical nature of how external communications interception works means that you cannot access that without accessing—intercepting—100,000 other e-mails going in the same direction or from the same region as well. That, to me, is a disproportionate interference. It may be justified to seek out that one particular person's e-mail, but if the only way in which you can obtain that particular e-mail is by intercepting a million other e-mails at the same time, it falls to be disproportionate. However valid the investigation may be, you can't justify that, just as you can't justify knocking down 100,000 doors because you want to find one murder suspect.

Emma Carr: This goes back to the original question about whether RIPA needs to be updated. I think the specific definitions need to be updated. We definitely need some definition of geolocation data in there, and I believe there is an issue about subscriber data held by service providers and the distinction in relation to a private but person-to-person communication—external versus internal. I think that when RIPA was first created, two British citizens e-mailing each other, one via Gmail and one via Yahoo, and that being described as an external communication was never the intention of the writers of RIPA.

Hanne Stevens: It is not just the entire overhaul of RIPA that concerns us, certainly. It is also reform of the Investigatory Powers Tribunal, which must, I think, happen also. Currently, I would say that the individual has no redress or remedy beyond the IPT, which is obviously closed, if they feel that they have been unjustly intruded on, and this seems to me a very untransparent and unjust way of doing things. There needs to be not just an overhaul of the legislation, but reform of the IPT.

Q42 Lord Butler: You have not mentioned the borderline between communications data and content. Do you think that RIPA also needs to be updated to draw that distinction more clearly?

Isabella Sankey: Yes. The distinction could best be explained and was more credible in the age of postal communications, when the communications data was the address on the front of an

envelope and the content was the letter inside. In the internet age, the distinction no longer stands up, particularly given our current levels of use of the internet, electronic telecommunications and so on. Communications data can build up as intimate a picture of somebody's life—their thoughts, their habits, their friendships, where they go, their medical records, their political affiliations, their sexuality—as reading the content of their emails or their letters. RIPA does not recognise that in all sorts of ways, not least that the acquisition of communications data does not require individual suspicion and does not require anything like the kind of authorisation that an individual interception in the UK does.

Q43 Lord Butler: Would you go so far as to say that communications data needs the same protection as content? In other words, that it needs to be warranted?

Isabella Sankey: Yes. We believe that all the intrusive techniques permitted by RIPA need to be individually warranted and that that must be a role exercised by the independent judiciary.

Chair: We have less than 10 minutes left and we would like to have your views on both oversight and transparency. Let us start with oversight.

Q44 Mr George Howarth: These sorts of activities by the agencies involve Ministers in the first instance, either through tasking or, as we have already discussed, warrants. Those are then reviewed and audited by judges and finally, if there is a complaint, it is heard by a special tribunal of judges. I think we know that all four witnesses don't think Ministers are the right people to sign warrants so we do not need go into that again. In those three stages, how do you think this system needs to be changed?

Dr Metcalfe: The current system of oversight for interception and access to communications data is conducted by the interception of communications commissioner. He gave evidence to the Home Affairs Committee that in 2012 he looked at 5% of interception warrants and most recently, in 2013, he looked at under 25% of interception warrants, which I think is really the high watermark. It has never been suggested that any interception commissioner has looked at more than a quarter of the interception warrants made in a particular year. Now imagine if a judge had said that they did not actually look at three quarters of the applications for search warrants. Imagine the outcry that we would have in this country, and yet we have a system of oversight where maybe as few as one in 20 warrants that are made by a Secretary of State are not looked at by anyone who is independent or impartial. That is simply not an adequate system.

I do not mean to criticise the interception commissioner or suggest that he is not diligent and conscientious—he is, of course, a retired Court of Appeal judge. I think there has been a substantial improvement in the quality of his annual reporting over the past two to three years, but it is plain that he simply does not have the time or the resources—he does not even work full time, for example—to look at all the interception warrants that are made. There are somewhere in the region of 2,500 interception warrants and somewhere in the region of 500,000 authorisations to access communications data. He has nine inspectors to help him look at authorisations for communications data, but even they do not look at more than 10%. It is a highly unsatisfactory system of oversight from the get-go.

Emma Carr: Resource is very important, but the commissioner made it very clear in his report this year that the transparent information that he believed should certainly be in his domain if not the public domain is simply not being recorded yet—for example the number of individuals that are put under surveillance and the types of offence. We see that frequently within the United States and that is all on public record, but it is not in this country. Until we start getting into that habit, not having it leads into the problems with oversight and lack of redress as well.

Q45 Mr Howarth: You are basically advocating something like FISA courts in this country?

Dr Metcalfe: FISA courts are a prior authorisation procedure for the most part. You can look at the way in which oversight, which is after the fact, works hand in hand with prior authorisation. There is an argument to be said that if you have a lot of judges, or a pool of judges, authorising all warrants up front, then perhaps a system where not every warrant is necessarily inspected after the fact is all right. There is a lot to be said for the judge who authorises a warrant continuing to have oversight as time goes on. It is a very common system under, for example, title III interceptions under the United States model.

Isabella Sankey: It is the pre-judicial authorisation that is so important.

In certain regards, it is not much use to the person whose privacy may have been hugely infringed if all they have is a declaration after the fact by the IPT—not that that happens very often. Eric gives the example of search warrants. In every other area where the state is able to infringe on privacy in this way, you have pre-judicial authorisation. It is most definitely the case that you can glean just as much information on somebody by bugging, intercepting or acquiring their communication data as you can by searching their premises, so why not have an equivalent form of protection?

Q46 Mr Howarth: Your belief presumably would then be that the commissioner's role should be to examine after the event every warrant that is executed, rather than just a sample.

Dr Metcalfe: Certainly in the situation where you do not have prior authorisation by a judge. For every single warrant, an authorisation must be looked at by a judge after the fact, which seems basic to me. I agree completely that the real issue is prior authorisation. If you have prior authorisation and continued oversight by the individual judge, then perhaps it is more acceptable to have a situation of more general oversight looking at the policies, procedures and so on.

On a further point about the Investigatory Powers Tribunal, in the first 10 years of its operation it upheld 10 complaints, five of which were from members of the same family.

Isabella Sankey: And concerned a local authority that had already admitted to the surveillance undertaken.

Dr Metcalfe: If you are not notified that you have been the subject of an intrusive surveillance operation, why would you bother making a complaint? By contrast, many people who are convinced that they are being constantly spied on by MI5 write a lot of complaints to the Investigatory Powers Tribunal. As far as the IPT is concerned, everything is fine, because it is going to receive many complaints from people who are writing in green ink, so they can dismiss most of them and uphold a very small number. It does not give you an accurate picture of whether in fact most of the surveillance warrants and authorisations made in this country are compatible with the necessary and proportionate principles identified by the European Court of Human Rights, because most of them have never been made the subject of a complaint.

Chair: We only have a couple of minutes left and I want the Committee to hear your views on transparency.

Q47 Lord Butler: We all agree that there must be an element of secrecy on the part of the agencies and the police, but there is also a general feeling that there should be more transparency. Could you give us any specific suggestions about areas in which you believe there should be more transparency?

Hanne Stevens: In relation to the IPT, there should be an appellate layer or upper tribunal. From the examples that we have just heard, it is largely ineffectual, unjust or any word that you wish to choose. How it is currently operating does not seem effective, so it needs reform, scrutiny and an upper tribunal to appeal matters to, so that individuals can have some form of redress or response or answer to why they have been intruded upon.

Isabella Sankey: We absolutely agree with that and would add that the IPT could be reformed to allow oral hearings unless there is a pressing reason for such hearings not to be allowed.

Complainants should also be notified when a hearing is taking place, which does not currently routinely happen. Reasons should also be given when a finding goes against a complainant. At the moment, a complainant is just told, "No. Your claim has not been accepted." We also think that transparency could be aided by notifying those who have been subjected to surveillance but are no longer, so that they may be able to challenge whether the surveillance was justified, necessary and proportionate, which I think is what Dr Metcalfe was just getting at.

More broadly on transparency, we of course accept that much of the work of the security services and indeed their capabilities need to be secret and that there needs to be a high degree of confidentiality. The service could not operate if that was not the case. What we object to is the notion that a mass expansion in the scale of, for example, the interception of bulk data is a capability. It is actually a huge shift in the nature of the work that the agencies undertake, so the idea that this is just a new capability or technological device that the public cannot know about is fundamentally flawed as a premise.

We would also say that the emphasis has to be much more on checks and balances, rather than greater transparency. If you have sufficient checks and balances in place of the type that we have just described, public trust and confidence can be enhanced and we can know institutionally that oversight is taking place as it should. That reduces the concerns that give rise to the need for greater transparency.

Chair: Thank you very much. We have sadly run out of time. On the behalf of the Committee, I thank you for your evidence. You have been very clear, helpful and positive in your comments, which will make an important contribution to our work. If you want to make any further comments, we will obviously be happy to hear from you in due course.

11:15 AM

The session concluded