INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

PRIVACY AND SECURITY INQUIRY

PUBLIC EVIDENCE SESSION 7

UNCORRECTED TRANSCRIPT OF EVIDENCE

Evidence given by:

The Rt. Hon. Theresa May MP
The Home Secretary

Wednesday 15 October 2014
(10.30 – 11.30)

Q1 Chair: This is an evidence session of the Intelligence and Security Committee of Parliament, and we are delighted to welcome the Home Secretary.

Home Secretary, this is the seventh public session—we have also held a number of private sessions—of our privacy and security inquiry. We are very grateful to you for your willingness to attend and answer our questions. As I think you are aware, the next hour will be a public session. Later in the morning we will move into a closed session, when we will deal with classified material. We hope this will be a very informal and relaxed exchange. We have raised a range of issues with other witnesses, and we are anxious to know your view, and the view of the Government, on those matters.

My first question is fairly general. The Government's submission to the inquiry states, "The first duty of any Government is the protection of its citizens…This includes the right to privacy and freedom of expression, as well as the right to personal safety and the right to life." From the Government's point of view, and from your point of view as Home Secretary, are those in any particular order of priority, or are they all to be seen as of equal importance? In that case, how do we deal with these matters in relation to intelligence capabilities?

Mrs May: Thank you very much, Chairman. I would hope that the statement stands by itself. I would not want to prioritise within that because, at any one point in time, when dealing with issues one looks at a variety of aspects of the protection of the citizen. Of course, when one looks at issues such as the rights to privacy and to freedom of expression, they are not absolutes. They have to be qualified if one is to be able to protect those rights, and the right to life, for people more generally. Sometimes it is necessary for the authorities to act in a way that is contrary to privacy, to interfere with somebody's privacy, in order to ensure the greater privacy and right to life of the vast majority of citizens.

Q2 Hazel Blears: What would you say to those people who are not convinced that that balance is struck in the right place and who allege that, at the moment, the country is subject to mass surveillance through bulk collection? What would you say to convince them that the ECHR right is very important but is obviously qualified, particularly for national security?

Mrs May: The first thing I would say is that the country is not subject to mass surveillance. There has been a lot written about this which is not accurate in terms of what the agencies undertake in order to keep us safe and secure. So that is the first point. The second point is that these issues of balance are ones which are constantly being looked at. Part of our democratic process is that these will be challenged, and it is right that Government makes its argument, and decisions are taken, about the level at which these issues should be taken. That is exactly what this inquiry from this Committee is about—it is part of that process. But I would also argue that, at the moment, we are subject to a significant threat, and it is right that Government takes the actions that are necessary to be able to protect citizens and to protect the right to life.

Chair: Thank you. Let us now move from the generality to more specific areas of questioning. The first is with regard to what is often referred to as targeted intrusion. We have taken evidence from all the previous witnesses, and there seems to be a broad consensus, including among many who have criticised other aspects of the intelligence agencies' operation, that targeted intrusion is a necessary element, even in a free society, but we do have one or two points we would like to raise with you in this area.

Q3 Mark Field: There is obviously a level of public scepticism about the signing of warrants. How much guidance do you take as Home Secretary in relation to that? In rough and ready terms, what proportion of the warrants that are put before you would you refuse to sign annually?

Mrs May: The number of warrants that I would refuse to sign would be very, very small. Just to set it in context, any warrant that reaches my desk, of course, has been through a very thorough process, in the agency that is submitting the warrant, but also in the Home Office. It goes through several iterations of consideration in the Home Office, so there may very well be warrants that have been sent back from the Home Office before they even reached me. Once they reach me, they should have been through a very, very thorough process anyway.

I do question warrants: sometimes I will question maybe the proportionality of a warrant; sometimes I will ask for some more information which will help me to make the decision. Often it is said that it is the thing that takes most of my time. I think, proportionately, if you looked at the whole of the Home Secretary's time, actually doing the red box is the thing that takes most of most Cabinet Ministers' time. But, no, seriously, in the Home Office, the amount of time I have to give to it each day is significant. I think that is important, and I do defend the process we have, because I think it is important that that decision is taken by somebody who is democratically accountable to the public.

Q4 Mark Field: Given the fast-changing world of the internet, technology and the like, and the fact that there are ever-greater potentially intrusive capabilities, do you keep an eye on exactly what is being asked for, as well as the particular facts of an individual's case?

Mrs May: Yes, and, obviously, there is a separate process of being made aware of the different capabilities that there are and being able to question those capabilities. But, in any case, on any particular warrant, it will be looking at what is being asked for and how that is going to be undertaken, against the case in relation to the particular individual. And, of course, I am signing warrants that are not just about national security in the terrorist threat sense that people think about, but also warrants from the National Crime Agency in relation to serious organised crime.

Q5 Lord Butler: May we deal with a topical story that does not involve warrants, although some people might think it should? That is the suggestion that the police have been pushing their

powers unduly—some might even say abusing them—particularly in seeking the sources of journalists. That is something they can do under RIPA without a warrant and self-authorised, as it were, within the police service. Are you satisfied with that situation, or do you think it needs to be looked at?

Mrs May: Well, it is something that we will be taking some action on, in the sense that we are going to publish a new code of conduct—code of practice—in relation to RIPA and in relation to the question of the use of these powers against certain sensitive professionals, which will include journalists. It is an issue that came up during the DRIPA debates in the House of Commons, and we undertook at the time that we would look at the code of practice and would issue a new one. I expect fairly soon to be able to issue a code of practice for consultation. It will cover this issue, which is about the circumstances and the sort of matters that have to be taken into account when considering particularly sensitive areas of intrusion, including in relation to journalists.

Q6 Lord Butler: But the code of practice, certainly under present legislation, would still mean that it was within the police's powers, subject to the code of practice. There is not a suggestion at the moment that a higher authority should be needed for that sort of intrusion?

Mrs May: At the moment, I am looking at the code of practice and what we can do through that to ensure that the police are making the right judgments, and that the right considerations are being taken into account.

Chair: We move now to what is perhaps one of the most controversial issues in this whole debate—the issue of bulk collection. Quite a number of our witnesses—not all, but quite a number—have said they object in principle to bulk collection, asking why it is necessary or appropriate.

Q7 Lord Lothian: As you know, Home Secretary, what is colloquially known as bulk collection has been described by the agencies as collecting a haystack of communications and personal data, and then searching that haystack. We have been told that the searches of the haystack are carefully targeted; they do not randomly look at any communications. They fire searches designed to meet certain specific criteria, and then they draw out the communications that meet those criteria and that are likely, therefore, to be of concern. The first question I have for you is: do you have concerns about the haystack itself, or are those concerns mitigated by the fact that the searches are targeted?

Mrs May: The description of the haystack is a good one, because if you are searching for the needle in the haystack you need to have the haystack in the first place, in order to be able to look for that needle. Therefore, what is important in this is the mitigations: the targeting; and the processes that are gone through to ensure that this is not just some sort of random mass surveillance, of the kind the right hon. Lady mentioned earlier. There is a necessity of having the material in order to be able to search it in a very targeted way.

This ability to have large amounts of communications data is important. We cannot emphasise enough that the collection of bulk data is not mass surveillance, precisely because what happens is this targeted process, which means this is not about just some sort of mass look at everybody's data. Most of the data will not be looked at at all; it will not be touched.

Q8 Lord Lothian: Leading from that, certain witnesses have suggested to us that bulk collection itself is an invasion of privacy. I wonder whether you consider that the privacy considerations bite at the point of collection, or whether they only bite at the moment when the communication is open.

Mrs May: I would say that they bite at the point at which the communication is open. For a start, if you take the view that you cannot collect bulk data, then you would significantly reduce the

ability of agencies and others to do their job, in terms of being able to target particular individuals and so forth, but I do not think the very collection of bulk data itself is an invasion of privacy. And I would say to those who say that that putting together a lot of data about individuals is not something that is restricted to the Government in some shape or form, and here we are talking about agencies in relation to national security. There are many commercial companies out there that put an awful lot of information together about individuals, which arguably is also an invasion of privacy, where they are looking at people's patterns of buying, for example, in order to target campaigns at them. So I do not think it is that collection itself where the privacy touches; I think it is at the point at which you are looking at that particular communication.

Q9 Lord Lothian: Do you think there is a general justification for bulk collection—it could be inferred from the answer you have just given—or do you think it depends on the nature of the threat that the bulk collection is meant to meet?

Mrs May: If you are saying to me, "Should Government just collect bulk data if it has no need to be able to have access to it for a particular purpose?", I do not think that the collection of bulk data itself, in an abstract form, is necessarily what Government should be about. Government should be about saying, "Where do we have a haystack in order to be able to access the needle that is necessary to keep people safe?"

Q10 Hazel Blears: The evidence that we have taken from many of the civil liberties organisations shows that they take a contrary view to the one that you have expressed. They feel that the collection of the bulk data itself is an intrusion into the privacy of all these people whose data it is even before it is searched, which is a clear differentiation. I asked them whether if it could be shown that the collection of bulk data and then targeted analysis actually developed targets that meant that we were then able to disrupt plots that saved people's lives, would they still think that the collection of bulk data was a step too far and should not be allowed. Almost unanimously, they said yes, so that is a clear position.

Is it possible to show some examples of how the process actually protects national security in order to convince the public on this? What ideas do you have? Some of the evidence from America has been that the collection of bulk data is not necessarily that effective. If we are going to do something that some view as a significant intrusion, the need to show that that is effective is quite important. What thoughts do you have on how to do that?

Mrs May: You raise an interesting point, because there is a need for all of us involved in decisions in this sort of area constantly to be thinking about whether we are informing the public sufficiently about what happens and how people do things such that they can have that confidence. In a separate example, I gave a speech a few months ago in which I actually talked about warrantry in a way that had not been done previously to try to get across to people exactly what the process is and how it is done.

I do not have an immediate answer to your question, but you have raised an interesting point. It behoves us to go away and think about whether there is scope for doing that in a way that is not threatening in national security terms but could give people greater confidence in what is done.

Q11 Chair: It might be of interest that one of the concluding comments of the retiring chairman of the National Security Agency in the United States was that he believed that they would seriously have to consider sharing information with the public that they would previously have thought inappropriate in order to win the confidence that they felt was necessary for them to do their job. Would you say that that is a similar consideration that will have to be thought about in the UK?

Mrs May: We have already seen a number of ways in which we have crossed barriers that in the past were thought to be absolutes, such as the very fact that this Committee now takes public

evidence from the agency heads, which five years ago people may have considered as something that definitely should not happen. There is a general recognition that we do need to be thinking about what information people can be given to give them that confidence in what the Government, in collective terms, are doing.

Q12 Fiona Mactaggart: Does that mean that never confirm, never deny needs to go?

Mrs May: No.

Q13 Dr Lewis: I want to come back to the evidence that we heard earlier, both from academics and from campaigning groups. When Hazel put her key question, which is, "If you could be satisfied that the collection of bulk data and its interrogation stopped serious plots and saved significant numbers of lives, would you still want the collection itself to be banned?" the campaigning groups were reluctant to answer the question, but eventually did and said yes. The academics were more willing to answer the question and also said yes. Interestingly, however, the campaigning groups, in seeking to avoid facing up to that really difficult choice, did make a number of arguments about the process. One, as we have heard, was that you do not get enough leads from it. The other was about opportunity costs and that the effort put into collecting bulk data would be better spent on targeting selected groups and individuals. What do you have to say in response to those two objections?

Mrs May: I go back to the answer I gave earlier, in that that the ability to interrogate bulk data—the ability to look for that needle in the haystack—is an important part of the processes that people go through in order to help to keep us safe. You are tempting me down the road of trying to give you some figures of actual cases and so forth, which is very similar to the question I have just been asked. The issue for Government collectively is the extent to which we need to explain to people how things are done, how it is possible to reach a position where somebody is stopped from a terrorist plot and what processes have contributed to that, such that people can see—

Q14 Dr Lewis: People can understand the theory, but the question is: how many times does it actually work in practice, compared with targeted surveillance? That is what people want to know. Surely we can release some statistics on this.

Mrs May: I would not commit to releasing statistics. We certainly need to look at what information is available to people such that they understand what is happening and how things are being undertaken, so that they have greater confidence in those things. Obviously, we always need to be careful about information that is released. The idea that there is simply an either/or in this—it may very well be that for the work that you need to do, you need to be able to find the needle in the haystack first.

Q15 Mr Howarth: I want to return to this issue of the state versus commercial organisations in terms of holding bulk data. Some of the people who have given evidence have argued that the distinction is that the individual enters into a transaction with a commercial organisation, and even though they may not have read the terms and conditions of that transaction, it nevertheless is a transaction that they have consented to. On the other hand, what the state does, although it may be legally justified, is not something that the individual concerned has any say over. How would you respond to those who say that?

Mrs May: My response would be that I think there is not a contract entered into, but an unwritten agreement between the individual and the state that the state is going to do everything that it can to keep them safe and secure.

Q16 Sir Menzies Campbell: I want to put an illustration to you, Home Secretary. There is a rather crude distinction between process and substance, and of course in the area of intelligence gathering, sometimes to reveal process can be very detrimental. The mere fact of the knowledge of how the agencies go about their work can be of enormous assistance to someone of malign intent. I have in mind the fact that in the past few months, all three of the agencies have talked about the threat that you mentioned a moment or two ago in quantitative terms. They have talked about several hundred areas, or even individuals, from which threats might arise. I wonder how far you think that boundary can be extended so that there is more understanding and more knowledge without prejudicing the very special characteristics that the agencies have to develop and implement in the course of their work.

Mrs May: This goes back to the question I was asked earlier. A constant challenge to Government is to find the balance between those two—between ensuring that there is sufficient information available to people that they have confidence in the processes and in what is being done in their name, but on the other hand not stepping over that boundary so that what is given out can be detrimental precisely because it gives away capabilities, or it gives away sufficient information for the people who want to do us harm to be able to work out what they should do in order not to be caught or stopped from doing what they want to do. I am not sure that I am in a position to give you an immediate response of: "Here is a different boundary from where we are today," or "This is the boundary we need to keep to today." It is a question about which we constantly need to ask: is there more that we can say in relation to it? We do it in things like communications data discussions, for example. We explain that this was a major part in dealing with terrorist threats and, indeed, in dealing with serious and organised crime as well. So I think the information that has been given out has increased over time, but we constantly need to look at that point.

Q17 Lord Butler: As has been said, the arguments of those who are opposed to mass collection are partly those of principle and partly utilitarian—it is not worth it—but if I may go back to the argument of principle, it was said to us that collecting bulk data is like holding DNA universally. You hold DNA and do not interrogate it unless there are some grounds to investigate a particular crime, and that has been found contrary to human rights. Why is the collection of bulk data similarly not contrary to human rights?

Mrs May: I take the view that there is a difference between the sort of information that you are dealing with when you are dealing with DNA versus information about people's communications, in the sense that the nature of DNA is in relation to an individual: it is not something that somebody has done, but is something that is intrinsic to that individual and is an essential part of that person. Obviously, as a Government we took a view on DNA.

There are some—one of my parliamentary colleagues does—who argue that the Government should keep an entire DNA database of everybody in the UK. We take a different view. In fact, we have restricted that, partly off the back of a court case which challenged the amount of DNA the Government were holding. So we have taken a particular view on that. I think that DNA is different, in that it is intrinsic to an individual. It is not something that somebody has chosen to do.

Q18 Chair: Before we leave this general section, could I just come back to you with a question that is based on what a number of my colleagues have been putting to you in the past few minutes, on how much the Government will be prepared to authorise openness about what bulk collection has achieved, in terms of protecting the public over the years—if that is the Government's position? Most of the statements you have made so far have been with regard to more openness about the process or you have been giving general statements, saying, "This has been effective", "This has been successful", "It is very important", and so on.

Such is the question mark about the degree of confidence felt by the public that there has to be a perfectly persuasive argument that it may be appropriate to go further. You referred to the fact that there has been much more openness since the 1990s about the role of the intelligence agencies and what they do, and about the nature of the threat. It is difficult to argue that any of that openness that has been achieved already, which is substantial, has damaged national security. There is evidence that it has reassured many members of the public that the agencies work in the public interest.

What I am putting to you, which I think echoes what has been said in the Committee as a whole, is that the issue of bulk collection is a relatively new one; the capabilities are relatively new and have all emerged in the way we see them today in the last 20 or 30 years, so perhaps general assurances of their utility are no longer adequate, particularly in the light of recent controversies. Are the Government willing to look, with a very open mind, at how far it might be appropriate to enable the agencies to actually give hard information—obviously, within the necessary constraints—about achievements that have already been delivered, to help this matter be taken forward?

Mrs May: On that general point, what I am certainly willing to do is, as I have said, take away the issue about whether there is more we can be saying about this that will give further reassurance to the public, but will not damage national security in terms of talking about capabilities. I am certainly willing to take that essay question away.

Chair: Thank you very much, it is very generous of you to say that.

We now turn to legislation. Mark, would you like to lead on this?

Q19 Mark Field: Obviously, the DRIPA legislation, to which you referred earlier, is very much seen as an Elastoplast to get us through a particular set of problems and will sort of self-destruct at the end of 2016. Therefore the coalition was firmly committed to an all-party review of RIPA in the course of either the remaining few months of this Parliament or in the early part of the next Parliament. Is this a tacit admission that RIPA is now not fit for purpose?

Mrs May: No, it is not. I think that RIPA is still good legislation that is still working well, but I think that it is a recognition that a number of issues have arisen that need to be addressed. Some of those issues are outside RIPA and are about the general issue of the powers that are necessary. Against the background of the threat that we face, what powers are necessary? What should be the arrangements for the exercise of those powers? So it is not just about RIPA: it is about the wider context in which the work is being done. The process, as I see it, is the David Anderson review, which will lead into what can be an all-party consideration of these matters after the election with the benefit of David Anderson's work.

Q20 Mark Field: Hopefully our review will play a small part in that consideration, too.

Mrs May: Indeed. There are a number of reviews.

Q21 Mark Field: I can see that other things are concerning you this side of an election, but do you think that given the rather piecemeal nature of this, and given the importance of public trust, it has clearly been undermined to a certain extent by the Snowden revelations and the fact that there has been such rapid technological change? Would you be open-minded to the idea that maybe the time is right for a consolidation of the legislation to bring a lot of these threads together and to level with the public about the importance of the work done by our security services, thereby making the case for why there has to be ongoing intrusion?

Mrs May: We have obviously had DRIPA, and we have already announced that we will be bringing forward further legislation with some more powers to deal with some of the issues that we now fear have arisen as a result of what we are seeing, particularly in relation to Syria and Iraq. I recognise that we have a number of pieces of legislation, and the reviews may very well come out

and say that what is needed is a consolidated piece of legislation, but that is something for us to see from the reviews.

Q22 Dr Lewis: RIPA provides for interception in what is described as "the interests of national security." What does the term "national security" mean? Is it deliberately intended to be a catch-all term to justify widespread surveillance?

Mrs May: No, I don't think it was drafted in the sense of feeling that, somehow, if one used this term it would be a wide-scale capability that would, in some sense, be misused. National security has a variety of elements, but at its core it is about the safety and security of the British people, of people living here in the UK and of UK interests.

Q23 Dr Lewis: It includes defence issues, terrorism and, rather more controversially, economic well-being.

Mrs May: When DRIPA was going through, we clarified that it was economic well-being in the sense of national security, because the term is obviously used in these contexts. Economic well-being obviously covers a number of aspects, but at its core it is about the safety and security of the UK.

Q24 Dr Lewis: But it makes a geographical distinction between people who are in the UK and those of any nationality who are overseas. What is the justification for giving less protection to people or bodies that are based overseas?

Mrs May: Obviously it does differentiate in terms of the requirements and the aspects of the Act that will be used to access different types of information. There is a difference between the sorts of work that are done under 8(1) and 8(4)—8(4) being the external part of RIPA. There is a difference in the sorts of issues that are being looked at and the perhaps more investigative aspect of 8(1). There will also be a difference in the information that is available in relation to people who are outside the UK versus people who are inside the UK.

Q25 Dr Lewis: But the idea is that, basically, if someone is inside the UK, you have a higher bar to clear before you can engage in surveillance than if you are dealing with people or bodies outside the UK.

Mrs May: But there is a slight difference in the nature of the work being done in relation to 8(4) versus 8(1).

Q26 Dr Lewis: Finally, on the basis that RIPA does not distinguish on grounds of nationality, what is the justification for UK nationals not having the same legal safeguards when they are abroad as when they are in the United Kingdom?

Mrs May: In terms of what we have just been talking about—the operation of different aspects of RIPA—I would go back to the point I just made. The essence of 8(4) and 8(1) is subtly different in terms of the work being undertaken.

Q27 Dr Lewis: Do you feel you can expand on that a little bit more?

Mrs May: Are you saying to me that if somebody is a UK national overseas, any surveillance or action undertaken under RIPA should somehow be done under an 8(1) type of warrant rather than an 8(4)?

Q28 Dr Lewis: The two types of warrants make different demands in terms of what tests have to be passed before the surveillance can be instituted. The demands made for carrying out surveillance within the UK are significantly higher for external targets. What I am saying is that you have a situation in which a British person is overseas and is likely to be more easily examined than if they were in the UK. Is there a justification you feel you can share with us?

Mrs May: The reason I mention the difference in what you are doing with 8(4) and 8(1) is that I think it goes to the heart of what you are saying in terms of intelligence gathering versus a more investigative tool.

Dr Lewis: Thank you very much.

Q29 Lord Lothian: I think RIPA allows for the targeting of classes of people. Do you think that is justifiable, or should it be restricted just to named individuals?

Mrs May: No, I have no problem with the abilities in RIPA at the moment in terms of what it enables to be done.

Q30 Lord Lothian: A number of our witnesses have suggested to us that because this invades privacy, the individual should be targeted rather than a category, for instance. Do you have a view on that?

Mrs May: There will be circumstances in which it may be necessary to undertake surveillance in relation to a group of people—in a very fast-moving situation, perhaps, there is a group of people—rather than being able just to target one individual. Sorry; I am not sure whether I have understood the nature of the question.

Q31 Fiona Mactaggart: I don't know whether this might help. Can you reassure us that a "group" would not include, for example—in a sus law sense—"people who are Muslim who live in this neighbourhood"?

Mrs May: Absolutely not. No.

Q32 Lord Lothian: I think we have taken that as far as we can. The other area I wanted to mention to you is the question of the distinction between data and content. A number of witnesses have suggested to us that with the development of the internet and internet communications, that distinction is becoming very blurred at best, and that possibly you get as much information from data as you might get from content. Do you think the time has come for pursuing data to have the same level of authorisation at ministerial level as pursuing content?

Mrs May: No, because I still think there is a distinction between data and content, and I think it is right and appropriate to have different processes and different levels of authorisation for the nature of those. I think we all accept that the intrusion of privacy with content is different from simply the communications data. Yes, it is obviously the case that as people communicate in a whole variety of different ways, it is necessary to upgrade the ability to access that communications data, but I do not think we have reached the point at which you can say that data is now so close to content that you have to have the same process for both of those. I think they are still distinct.

Q33 Sir Menzies Campbell: I will not rehearse again the things that Julian Lewis said a moment or two ago about sections 8(4) and 8(1), but am I right to infer from the answers you gave that you see the distinction, really, as being one of characteristic rather than principle; that is to say, the nature of the investigation in this country would be different from the possible investigation that was carried out abroad. Is that correct?

Mrs May: I think that the regimes are different because—and I have used the two terms—8(1) is an investigatory tool, and I used the term "investigation", whereas 8(4) is primarily an intelligence-gathering capability. So it is the case that the characteristic of what is being done under the two different warrants is by nature different.

Q34 Sir Menzies Campbell: So the answer to my question is that it is different characteristics, which allow—you would say—for a different approach.

Mrs May: I think they do allow for a different approach. Obviously, there is the externality—

Sir Menzies Campbell: As authorised by Parliament.

Mrs May: But also there is a different characteristic, yes.

Q35 Sir Menzies Campbell: I wonder if I might take you to another question on this issue of "abroad". If you are conducting an investigation in the United Kingdom, then it is more than likely that there will be knowledge of an individual or individuals. If, on the other hand, you have received credible information of a threat from—let us be neutral—one of the intelligence agents of Ruritania, and the fact that there may be something in the pipeline, in the second case it would not be possible to be as targeted as in the first. In those circumstances, isn't it inevitable that the intelligence agencies would be looking for groups—would be, in a way, trawling—to some extent by comparison with the sort of activity we have discussed in the United Kingdom itself?

Mrs May: I certainly would not use the term "trawling", but I think as we have described the nature of the task will be different. When you have information about a specific individual who you may wish to be looking at because of concern about their intent and actions, that is different from perhaps a more general intelligence-gathering capability.

Q36 Sir Menzies Campbell: Well let us take the term "trawling" out of the equation and let me frame that question slightly differently. If you think it is the MI5 equivalent in Ruritania, then that is what you know, but you do not know which particular officer or officers may have responsibility for this project which would damage us, whereas in the case of the United Kingdom it is more than likely that one would have much more precise knowledge about the individual or individuals who are the subjects of concern.

Mrs May: Yes. The different picture you paint is a perfectly reasonable one, in which that may very well be the circumstance.

Q37 Mark Field: There is just a fundamental suspicion that we are able to arbitrage, to a certain extent, and because things are happening out of sight—perhaps out of mind—abroad, we can get rather more information, and therefore there is a preference in the intelligence services to go down that route and play a little bit hard and fast with the rules, rather than having to do it through domestic legislation, through the 8(1) route.

Mrs May: No. I mean, there is absolutely nothing that I have seen that would suggest anything of that sort whatsoever. I think these are recognised as different instruments and different processes—obviously, I deal with the 8(1) warrants—that reflect different scenarios; but there is no suggestion whatsoever that this is a sort of "Oh, well, why don't we use one of these because it is going to be easier". Absolutely not. I completely reject that concept.

Q38 Lord Butler: There is a suggestion, some of which may be misunderstanding on the part of witnesses, that the way technology has moved means that more things can be interpreted as external rather than internal. One example of that is the fact that so much of people's internet records, and so on, are now held on the cloud, which is held somewhere overseas. So much of it,

when it is between internal people, passes through external cables, and this may be exploited by the intelligence agencies. As I say, I think some of that may be based on a misunderstanding, and we will have to have technical advice on it, but I wonder if you have got any comment on it.

Mrs May: This is one of the issues that has been addressed in evidence that has been given to the IPT—a very clear description of the difference between an external and internal communication. I was just looking to see if I could find the very good phraseology—

Q39 Lord Butler: I think it was that evidence from Charles Farr that caused people to take up some of these points and raise some alarm.

Mrs May: Having looked at it, I really do not see why that was the case, because I think the intention of the legislation was absolutely clear from this.

Q40 Chair: Our understanding, Home Secretary—perhaps you would like to comment on whether this is the case—is that if a communication is sent from someone in the United Kingdom to someone in the United Kingdom, the fact that it may be routed through other parts of the world does not remove the need to apply domestic legal requirements for intercepting that information. It cannot be classed as external for the purpose of legal authorisation.

Mrs May: Yes. This is perhaps it: "Thus, an email from a person in London to a person in Birmingham will be an internal, not external, communication for the purposes of RIPA and the Code, whether or not it is routed via IP addresses outside the British Islands".

Q41 Lord Butler: Another argument that we have heard from some witnesses is that people under 8(4) need extra protection because they have human rights, too. It is not only people within the United Kingdom who have human rights; foreigners have human rights. Have you got any comment on that?

Mrs May: Of course, human rights are not restricted to people living in the United Kingdom. I come back to the point that what is being missed when people look at this is the essential difference in the nature of the tools that are being used.

Q42 Lord Lothian: I want to follow up on Lord Butler's question. This relates to the cloud, because a lot of people find that the content that they are dealing with is automatically transferred to the cloud, as I understand it. I am frequently being asked on my laptop whether I would like automatically to save all my photographs, and as I far as I know those are designed to end up in the cloud. The cloud, technically, is based in the United States, as I understand it. How many people in this country would regard their communications to the cloud as being external rather than internal, which is what the definition by Charles Farr suggests?

Mrs May: First of all—I am not in any way a technical person, so I am sure that this will need to be checked—my understanding is that not all of the cloud is in the United States.

Q43 Lord Lothian: The cloud is based, as I understand it, in California.

Fiona Mactaggart: Let us assume that a bit of it is.

Mrs May: I do not think that the concept of the cloud as just being one thing in one place is correct, so this is a more complicated issue than perhaps that would suggest. For somebody who sends their communication via the cloud to somebody else in the United Kingdom, you are right. They think that they are having an internal communication. According to the definition that I have

just read out, "an email from a person in London to a person in Birmingham will be an internal, not external, communication…whether or not it is routed via IP addresses outside the British Islands".

Fiona Mactaggart: But if you are putting a photograph into the cloud, that is not an e-mail sent to somebody. That was the example that Lord Lothian gave.

Chair: I think we may need to get more technical advice on this matter rather than expecting either the questions or the answers to have that degree of technical expertise.

Mr Howarth: I think it is about legal jurisdiction rather than physical location.

Chair: It is a legitimate point. Perhaps, Home Secretary, you could let the Committee know in due course the response to Lord Lothian's question. It is an important point, but I am not sure that we are going to be able to obtain a clear indication here.

Mrs May: I think I need to take some technical advice on this before I respond any further.

Q44 Sir Menzies Campbell: I would not understand any distinction between a photograph and an e-mail; they are items of communication and I cannot see why it would be necessary to distinguish one from the other. However, you will no doubt be happy to share the technical advice you obtain, in case I am labouring under a misconception. A number of witnesses have sought to draw a distinction between post and telephone calls, compared with e-mails. Do you see any justification for a distinction of that kind?

Mrs May: I would say that a communication is a communication. People undertake it in a variety of different ways these days, but a communication is still a communication. I am not sure why they draw the distinction and what implications that has.

Q45 Sir Menzies Campbell: That is my next question. They draw a comparison between the volume of communication on the internet and its accessibility, which far outweighs anything that post or telephone calls can provide. They say that, because of that distinction, a different approach is needed towards communications data on the internet. Would you draw any such distinction?

Mrs May: I do not think that the volume of material which goes across the internet requires, in itself, a different approach to be taken.

Q46 Sir Menzies Campbell: What about the characteristics of it?

Mrs May: That is why I come back to the point that a communication is a communication. When you are looking at communications—as I indicated earlier—you are either looking at the raw data about a communication rather than its content or are looking separately at its content. You want to be able to do that whatever the means of delivering that communication. The fact that far more people will use e-mail and much more information will be available does not mean that you should not be able to access some of that under the same sort of strict conditions that you can access other communications.

Q47 Sir Menzies Campbell: What about the fact that communications on the internet remain—it is like that line: "The moving finger writes; and, having writ, moves on." What you use the internet for is permanent. Is there a distinction to be drawn between that and the kind of communication involved in a letter or telephone call? It is a permanent record of what you said or did at a particular time.

Mrs May: Some letters are there as a permanent record of what you said or did at a particular time, dependent on whether the recipient retains them.

Q48 Sir Menzies Campbell: Exactly.

Mrs May: No, I would not see that leading to a distinction.

Chair: Thank you. In our final eight or nine minutes, I want two questions on oversight and transparency.

Q49 Mr Howarth: Very helpfully, you have already answered one part of the question I was going to ask about the involvement of Ministers in authorising warrants. You have made it clear that you think that is right. Some witnesses have argued that, for reasons of technical expertise or the perception of independence, those decisions to authorise a warrant should be taken by either a judicial figure—a judge, for example—or someone with the technical expertise to deal with it, or maybe some combination of the two. Why do you think, because of the issue of accountability that you raised, that Ministers are the right people to do that?

Mrs May: I believe very strongly that when you are giving someone permission to intercept someone's communications, in whatever form that may be, or permission for some other action which is an intrusion into someone's privacy, it is very important that the person taking that decision can be directly accountable to the British people for it. That is why I argue that it should be someone who is democratically elected and I would certainly say that it should be someone who has a greater understanding of the wider context in which those actions are taken. If you have somebody who is just looking at it technically or legally, they might look only at the bare bones of something and not consider the wider context of the public's expectations about the extent to which this should or should not be possible. A wider understanding is important, but it is also important that people are able to look to see an individual—it is one of the reasons why I recently talked about warrantry in my speech, because it is important that people understand a bit more about this. That is why people should be able to say that, actually, yes, that is somebody who is elected and can be got rid of. Governments can be overturned if people are unhappy with how things are being undertaken; they cannot do that with a judge.

Q50 Hazel Blears: I want to talk about a very simple matter. The point has been made to us that, for example, you go to a judge for a search warrant, yet the kind of intrusion that you authorise through a ministerial warrant is equally serious, whether eavesdropping or electronic surveillance. What is the logic of the distinction between having a judicial authority for a search warrant but a political authority for other forms of intrusion?

Mrs May: There is a subtle difference, I think, in the type of intrusion that is taking place. If the police get a search warrant to go and search somebody's house, it is pretty obvious that they are searching somebody's house—they physically turn up and undertake the search of that property. The interception of communications is an intrusion of privacy that is not, by definition, "out there"; nobody put up a notice to say that it is happening.

Q51 Hazel Blears: If you are going to enter somebody's premises and install equipment, is that not very intrusive?

Mrs May: Yes, that is very intrusive, but, as I say, I would argue that the nature of the intrusion is slightly different, so it is important that the authorisation has democratic accountability to it, rather than it simply going through the judiciary.

Q52 Mr Howarth: Both the shadow Home Secretary and the Deputy Prime Minister have argued that the two commissioners should be replaced by an inspector general. Do you agree with Nick?

Mrs May: Obviously the whole question of oversight is going to be part of the work being done leading up to the David Anderson review and other reviews, including the work that this

Committee is doing. The Government looked at this previously and did not go down the route of having that single individual. There is an issue in the work that the commissioners do: I think that they do very good work, but they produce these reports that, sadly, very few people actually notice or look at. In particular, the last report produced by Sir Anthony May, where he perhaps went further than has happened previously and was starting to try to ensure that the whole role of the commissioners was seen rather more effectively, was an important step.

Chair: Finally, let us move on to transparency.

Q53 Fiona Mactaggart: There has been criticism that Ministers were not aware of what the agencies were doing and that members of the Security Council were unaware of bulk collection. Is that true? Did you know what the agencies were doing?

Mrs May: Yes, I certainly know the actions that are undertaken by—I have particular responsibility for MI5, obviously, because GCHQ and SIS are not within my particular remit, so I will be dealing in more detail with what MI5 does, rather than other agencies.

Q54 Fiona Mactaggart: So you feel thoroughly informed about what they are doing.

Mrs May: I do feel informed about what they are doing.

Q55 Fiona Mactaggart: That leads me on to the issue you just talked about: the expectations of the public and the fact that the Home Secretary is the person who approves surveillance of this kind. If the public do not know what the process is, how does that accountability work?

Mrs May: That is precisely why I have been trying to open up what the process is, tell people about it, explain that it is the Home Secretary who does this and that it is a significant part of the role, and actually get out there rather more what is happening.

Q56 Fiona Mactaggart: This comes back to my point about "Never confirm, never deny": Big Brother Watch said to us in their evidence that the convention that Ministers do not comment on intelligence matters is increasingly absurd. It becomes difficult when *The Guardian* is publishing the Snowden allegations and people are talking about whether or not the names of programmes are true, and the response to that from Government is silence.

Mrs May: No, I think that there are times when it is entirely right that the Government should be silent on things, which is why, when you asked me about neither confirm nor deny, I said that no, I do not think that it is the time to change that. As I indicated earlier, I think it is right that over time there is a constant process for Government of looking to ensure that sufficient information is made available to reassure people and give them confidence. I have just explained part of the warrantry process, which I am trying to expose more to the public so that they can see what is happening and understand it rather better. However, there will be occasions when it is entirely right for the Government to be silent. There will be times when, in a publicity sense, it would be in the interests of Government to be able to say something, but it is right that we don't.

Chair: Home Secretary, it follows naturally from what you have just said that our public evidence session must be brought to an end. As you know, we will go into closed session later this morning, when we will be able to question you further about areas dealing with classified material. Thank you for the evidence that you have given so far; we look forward to continuing the exchange.

11:30 AM

The session concluded