INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

PRIVACY AND SECURITY INQUIRY

PUBLIC EVIDENCE SESSION 6

UNCORRECTED TRANSCRIPT OF EVIDENCE

Evidence given by:

The Rt. Hon. Nick Clegg MP
Deputy Prime Minister

Wednesday 15 October 2014
(16:30 - 17:15)

Q1 Chair: I welcome you, Deputy Prime Minister, to this public session of the Intelligence and Security Committee. This is one of seven public evidence sessions that we are holding for our privacy and security inquiry, and we are delighted that you can be with us. We hope that this will be an informal session. I am sure that we will all have questions to put to you, but I begin by inviting you to make opening comments. We have, of course, seen the speech that you gave to RUSI, which was a helpful way of informing us of your opinions and thoughts on this important question, but if you would care to make any opening comments, please feel free to do so.

The Deputy Prime Minister: Thank you very much for inviting me to be with you this afternoon in the context of your inquiry on the vitally important issue of security, privacy and how we strike the right balance, not least in view of the enormous technological changes going on around us. I will make three opening observations, which I hope will be of some help.

First, I sometimes feel that quite a lot of the debate in this area becomes unhelpfully polarised, as if any additional measure to enhance collective security will always come at the cost of individual privacy and any step to enhance individual privacy will always come at the cost of collective security. That is self-evidently not the case; the relationship between the two is altogether more complex. You cannot have privacy unless you have security to enjoy the freedoms that we have in a free and open society. Equally, you do not create security in an environment in which citizens feel that their privacy is not safeguarded. I have never quite believed in a zero-sum game, or in the see-saw effect of the debate. I think the tension is more interesting than that, and that in many ways, we can seek to both enhance security and protect privacy. It is not always a crude trade-off. That is the first point I would make.

Secondly, as an old-fashioned Liberal, I think that the state should always be a reluctant intruder in this area. The ability of the state to intrude on someone's privacy in the name of collective

security and so on is an uncontested role, but it must always be applied on the basic tests of necessity and proportionality, held to proper account and subject to the right levels of transparency.

Again, if we keep that prism in mind, it is the most helpful way to deal with these issues. Often, it is not about whether the state has the right to seek to gather or analyse this or that information; it is about whether it is done in a way that is properly proportionate, bound by the tests of necessity and held to proper account. It is not least because the sheer volume of information involved has grown exponentially, certainly since we last legislated in this area through RIPA 14 years ago; it is also about the sheer multiplicity of the threats. Those are the tests and concerns that are always uppermost, at least in my mind.

Finally, although I am sure we will come to this, I have a feeling that because the level of technological innovation is so great and the volume of data is now so huge—I read somewhere the other day that more e-mails are sent in this country in four days than all the mail sent during the whole year; I think it was 1.3 trillion or something. It is of such unimaginably large volumes, and we did not confront that when we last debated it in Parliament and tried to set the legislative framework for this. I intuitively think that the scale of the information and the velocity of the technological change involved mean that a lot of old distinctions are increasingly being blurred, or possibly destroyed altogether. National or international is increasingly a meaningless distinction; domestic and international IT traffic are becoming synonymous. The distinction between communications data—what some people call metadata—and content is increasingly blurred compared with the debates we once had about this.

For those reasons, I increasingly question our ability to deal with some of these issues on our own. In other words, I think we will have to move, in time, towards a more treaty-based approach in which jurisdictions become more compatible with each other across the world. This is a global phenomenon, which needs some basic global disciplines and checks and balances, including, perhaps—this is rather a pious way of putting it—some sort of constitution for the internet, so that people who use the internet feel that there are certain parameters and certain rights that they can exercise in that space. Those are my first three fairly esoteric thoughts, which I hope are, none the less, helpful.

Q2 Chair: Thank you for that very helpful introduction. Can I lead with a question? Since the turn of the century, we have had two developments, which have coincidentally happened in parallel. We have had the serious growth in the terrorist threat to the security of people in this country; there were the 7/7 bombings but also many other plots, some of which were disrupted by the intelligence agencies themselves. Parallel to that, we have had what you have just remarked upon: this extraordinary technological revolution, which has made so many more things possible, from a technical point of view, for our intelligence agencies as they try to deal with this threat. Do you start from an assumption that—obviously, under law and with proper safeguards—the intelligence agencies should be able to use all the technological potential that exists to try to identify terrorists and potential threats, particularly as the terrorists themselves can sometimes be very sophisticated in their use of the same technology?

The Deputy Prime Minister: Yes is the short answer. You have to compete in the same space where the threat presents itself, and you have got to give the agencies the means to compete in that space, if I can put it like that. It becomes more complicated where you try to draw the distinction between going after individuals and seeking somehow to—this is the whole debate about bulk data versus warranted investigation, and the needle in the haystack and so on. That is where it becomes a lot more complicated.

Q3 Chair: Where do you come down in that debate?

The Deputy Prime Minister: From a pragmatic level, it seems to me that you cannot find the needle unless you have a haystack. When we last legislated on this—this is why although RIPA serves us well, it is right to ask questions about it—we did not, as a country, legislate for the kind of haystack that we are having to create.

Then there is the whole question of how long you keep that haystack, and the idea of inert data. Some people, who are at one extreme of the debate, say that just holding that inert data is already an act invasive of privacy, even if you are not scrutinising the data or doing anything with it. Other people say that it is an entirely innocent activity because—I am mixing my metaphors here—it is a great tub of data and you are not doing anything with it, and you go after something inside it only on a warranted basis.

My own view is that just by virtue of necessity, you need to create that receptacle of unexamined data that you then have to scrutinise, but it is not enough for the state simply to assert its right to do that. The state must prove its right to do that, and it is perfectly legitimate for us to ask questions about how long you hold that data, and how you can be absolutely sure that it cannot be put to more malign use. After all, it is data that is available, and you could imagine circumstances in which people were to get hold of it in less benign ways.

By the way, I should say on that, that having worked in the past four and a half years in Government as Deputy Prime Minister and seen the work of the agencies in this area, including, and most especially, GCHQ, I have absolutely no doubt at all that the people in the agencies work punctiliously and with great attention to their legal duties. I have never for one moment questioned their commitment to their legal duties. The onus is not on them to ask those questions; the onus is on us to ask ourselves whether the regulatory and legislative context in which we place them has kept up with events.

Q4 Hazel Blears: I want to press you a little more on this area, because we have had some fascinating submissions from a whole range of organisations, particularly civil liberties groups such as Big Brother Watch, Liberty and Amnesty. We pressed them quite hard to say that, on bulk collection, if it could be shown that by properly interrogating bulk collection we were able to identify targets, which then meant that we could prevent plots, would they still regard bulk collection as an unacceptable infringement of people's privacy, because that is their starting point? We pressed them really hard on that: that even if there was evidence that would stop plots and save lives, would they still regard that as unacceptable? And virtually all those groups said yes, they would.

The Deputy Prime Minister: Would what?

Q5 Hazel Blears: They would regard bulk collection in and of itself as such an infringement of people's privacy that it would not be justified, and you are now telling us that you take a different view in relation to bulk collection and you regard it as justified.

The Deputy Prime Minister: Oh, yes—absolutely. Unless someone else can show how we can go after the data that we are perfectly entitled to as a state in order to keep people safe or, in other words, how do you—I am sorry, I am just reworking the familiar analogy—create the haystack, without which you cannot go after the needle?

For me, it is not really so much an issue about whether that is just an unavoidable reality of how information is contained and framed at the moment. It is more a question of, "Have we anticipated that in the regulatory and legislative framework in which that data is collected?" There are a number of distinctions, as I intimated earlier, which are not explicitly dealt with by RIPA. So, the distinction between bulk data and content is alluded to, and of course what GCHQ does is entirely lawful, and in the terms of 8(4) warrants it is explicitly alluded to, but slightly in passing.

You have got this whole increasingly fungible distinction between communications data—kind of how you categorise data—and the content of data. Increasingly, a lot of experts—I am sure they

would have repeated this to you—tell us that actually it is the comms data that tells you as much as you need to know as content. And yet the hurdles by which the state justifies going after communications data versus content is much lower, as set out in RIPA. Is that appropriate to the way in which comms data, in many ways, has increased in its utility to us?

The distinction between external and internal—you and I could send an e-mail to each other, and it could be routed via a completely different hemisphere. Is that external communications, or is it domestic? Can GCHQ's external-facing mandate—unwittingly perhaps—actually end up covering what are, strictly speaking, domestic forms of communication?

All those things seem to me to have arisen as dilemmas since we last legislated on this; that is the point I would make.

Q6 Hazel Blears: There is much common ground there on all those issues that you have mentioned, but one of the sticking points for many of the people who have given evidence was that the actual act of bulk collection of data and content was an infringement of people's privacy, even though they did not know, and even though that information was never interrogated unless it was specifically targeted. The very act of collection was unacceptable, but you are telling us—and you have been very clear about it—that you do not subscribe to that view.

The Deputy Prime Minister: No. Absolutely. Let me be very clear: I have not yet seen a way in which we can ask our agencies to go after data, which they should do in order to keep us safe, without in some way doing so by first setting aside the block—a kind of granite block of data—in which they then interrogate the much more specific data they are after.

However, the point I am seeking to make is that there are very legitimate questions about how long you hold that sort of inert data, how it is held accountable, how it is scrutinised, how it is checked, how do you ensure that it does not in any way fall into the hands of people who might want to make use of it in a way that converts it from being sort of inert data into being actively scrutinised, and this external/domestic distinction comes into play as well. It seems to me that all those things need to be revisited, and indeed are being revisited by your inquiry and those inquiries held by others.

Q7 Dr Lewis: Going straight on from that, what you have said today is entirely consistent with what you said to the RUSI, when you said that, "The idea that the security services should be able to track communications in order to pursue or disrupt serious criminals and terrorists is not controversial. If, in order to do that effectively, the judgment is that there is no practical alternative to bulk data collection, then to some degree we should allow it."

The Deputy Prime Minister: Correct.

Q8 Dr Lewis: And that is what you said today. Just to play devil's advocate on the basis of the arguments we have heard against that: first, questions have been asked about whether or not there is an opportunity cost because the effort put into collecting bulk data detracts from the effort that might be put into more targeted surveillance with the same resources. Secondly, people say that they have no evidence that the collection of bulk data has actually resulted in the creation of many or any new leads that have prevented terrorist attacks. What are your comments on those two points?

The Deputy Prime Minister: On the first, I would say that of course the use of bulk data is not the only means by which the agencies can identify both data that is essential to keeping us safe and threats that need to be countered. There are of course a multitude of other ways—for example, human intelligence, or other leads where you can go straight to the person, their technology or their premises. All of that is set out in the warranted powers provided to Secretaries of State under RIPA. So it is not the only means, but in my view and from my experience of Government it is one legitimate means. From what I have seen, I am absolutely persuaded that there have been

circumstances in which it would have been impossible for agencies to interrogate specific data about specific threats without, in a sense, first having cordoned off the data in which it was situated, if I can put it like that. I am persuaded of that.

I will repeat what I said earlier: where I think there is a legitimate space for critics to ask whether we really have the framework right is on the retention, scrutiny, accountability and reporting of it all. Is that as strong as it can be? My view is that we can go much further. We have taken a number of steps, but we could take more.

Q9 Dr Lewis: So you think that the oversight bodies, including this Committee, could do more to satisfy the public that these techniques are necessary in terms of the results that we can be told they have obtained.

The Deputy Prime Minister: I would like to take a step back for a second, because I think this is relevant. It is a commonplace observation, but we live in a period of our history in which all forms of authority are treated with unbridled scepticism and cynicism. That is true of a doctor, a priest, a judge, or—perhaps most especially—a politician. Quite rightly, there is a very forthright sense of scepticism about how authority is wielded, particularly where it is wielded in the name of the public.

I desperately want to avoid a situation in which the agencies are constantly having to fight for their basic legitimacy. I have never seen increasing oversight or transparency as an enemy of the work of the agencies; I actually think that it is an increasingly indispensible part of ensuring that public confidence in their work continues. My personal experience is that there is a bit of a tendency to keep stuff secret that could easily be published without any harm. That is my view. We could unclench quite a lot when it comes to some of the data that could be published. A good example is that we know that about 500,000 communications data requests are made every year, but there is no data in the public domain about whether that is 500,000 individuals or 500,000 premises—it might actually be a much smaller number of individuals but lots of repeat communications data requests. The public are perfectly entitled to know that, and that is one thing that I hope will be published in the transparency report, the first of which I hope will be published before the election, as agreed as part of the measures around the rather unfortunately named DRIPA legislation.

We can be more open, and the improved powers of this Committee are an important component of that. As you know from my speech, my own view is that this Committee could be reformed and strengthened further through various means. I do not see any of those improvements as a threat to the legitimacy of the agencies—I would actually flip it right round and say that if you do not do it, you create the conditions in which public scepticism about what the agencies do only festers further.

Q10 Lord Butler: To pursue the bulk data point, which will be central to us, as Julian has said, one of the objections is a utilitarian one, that there is no evidence that it is effective in producing new leads. The other objection of principle is best illustrated by the issue of holding DNA universally. People say that the courts have found against holding DNA, even though you do not interrogate it unless there is some reason to do so. How do you distinguish between those two cases?

The Deputy Prime Minister: It is difficult, isn't it? ID cards are a similar example. One of the first acts of this coalition Government was to scrap the ID card database that had been established by the previous Government, on the basis that we felt the utility—there is undoubtedly a utilitarian case for coalescing a lot of information about one person on one identity chip—was outweighed by the concerns about privacy and the possible abuse of the honey pot of data that you create about individuals. We physically destroyed the database, and we certainly had the public on our side.

I am not pretending that people's reactions to these things are meticulously consistent because one thing that has been regularly observed and is self-evident is that people to be more relaxed about data that they provide to private sector players and operators such as supermarkets, retailers and so

on than to the state. I think that speaks rather well of the British people; they are a lot more sceptical about what the state is doing than what their supermarket is doing. They are in a sense right because the state ultimately has more untrammelled powers to invade the privacy of individuals' circumstances than the local supermarket does. But there is not complete neatness in these things.

I am persuaded but admit I might not be quite as persuaded as I am if I had not had the experience of being in Government for the past four and half years and seen the utility of what the agencies do. As I said before, I have seen the seriousness and meticulousness with which they take their legal duties and are conscious of their article 8 ECHR obligations, namely that there is a right to privacy under article 8, but not an unqualified one. My experience is that they try to balance these things.

I have come to the view that it is difficult to argue that it is possible for those agencies to do what any reasonable person expects them to do in the kind of data-rich environment in which they have to operate without to some extent—I stress to some extent—holding inert data that is then interrogated more precisely. If there were a way to square the circle no one would be more delighted than me. If everything could be done through an individual, monitored process, that would be great, but that is not how data presents itself now.

Q11 Lord Butler: The earlier version of the Communications Data Bill you could not accept, and it did not go ahead. We are told there is a new draft of the Bill. I do not know whether that is a Conservative party construct or a Government one. Can you tell us, and can you tell us whether there is a new draft to which you object less?

The Deputy Prime Minister: No, there is no recycling of the Communications Data Bill in existence, certainly not one that has been circulating in Government for collective discussion.

The Communications and Data Bill sought to do three things. First, to oblige internet service providers to retain for a year all the weblog activity history up to the first slash of any website that you or any of us had visited during a whole year. Secondly, to resolve the technical issue that the IP addresses are not individually matched to mobile devices any more. In effect, one IP address is being used by multiple mobile devices at the moment and that is proving difficult for law enforcement agencies. Thirdly, to make clear that there is an extraterritorial component to the request made by the British state and its agencies of the internet service providers, where we are fulfilling our duty to keep British citizens safe.

I have always said—I said it publicly at the time—that I have no problem at all with the second part of that; there is just an obvious technical issue where it is proving to be very difficult. There were some notorious cases involving threats to the lives and welfare of some children, which have recently been the subject of some public discussion, which were handled by the National Crime Agency. It is clear to me, having looked at it, that the specific problem, according to the National Crime Agency, was that they could not match the IP addresses to the device, and that is why they could not pursue the leads that they had. We must deal with that. I want us to deal with that and I hope that we will be able to present to Parliament shortly a legislative change that will deal with that problem.

The third of the three issues—extraterritoriality—is a little bit more complicated, but it has been partially addressed by the DRIPA legislation. We have made it clear that, when requests are made for data from internet service providers, the acid test is not where they are located, but whether the data that we want pertains to British citizens, whether that is those who threaten our safety here in Britain or British citizens who are under threat themselves. That is the clarification in the law that we made in the legislation just before the summer recess.

It was the first bit that I objected to so strongly, and still do now, because I do not think that it meets some of the tests that I talked about earlier. I do not think that the necessity or proportionality

was demonstrated at all. I think that storing the web record of every single individual in this country for a whole year was a disproportionate response to the challenge that it sought to address.

Sorry to give you a rather lengthy reply, but there is the slightly crude thing of: are you going to do the Communications Data Bill or not? I have always said that we should do one third of it—I am one of the leading proponents of it and I have recently expressed my slight frustration that we have not moved as fast on that as we should, given that, on my personal insistence, it was included in the last Queen's Speech. We have addressed in part the extraterritorial component, where there was an increasing risk of legal friction between internet service providers whose servers are located elsewhere and our legitimate wish, none the less, to extract or demand data from them. It was the first bit of that tripod of measures which I felt was disproportionate, and I have not wavered in my view on that at all.

Q12 Lord Lothian: You have raised important questions about bulk data, both in your speech to RUSI and today. I want to press you a little bit. You were talking about the extent of bulk data collection, the length of time it was held for and the criteria on which it should be justified. Do you see a general principle emerging that will deal with all three of those, or might it vary from circumstance to circumstance according to what might be the perceived level of the threat being pursued, or do you see them being set out in terms of particular lengths of time? Do you have any view on that? How much data could be collected? How long should it be held for? What should be the criteria?

The Deputy Prime Minister: I do not have a ready-made answer to that at all. In fact, one of the interesting things is that I have not come across anyone who has got an oven-baked solution to this; everyone is still grappling with this same dilemma. Actually, as I try to compare the debate here with that in the United States, France and elsewhere, I think that the level of debate here is already a lot more sophisticated than in other jurisdictions.

No other jurisdiction has come up with a neat answer for this either, but I think that this inquiry, the RUSI inquiry, the review by David Anderson of the RIPA legislation, and the commitment that we have made, given that the DRIPA legislation is on a short sell-by date—basically, it lapses at the end of 2016—means that we are on a self-imposed race against the clock to come up with an answer and I hope that we will be able to use the time between now and the general election, through these inquiries, to try to coalesce around a sensible approach. But no, I am not going to pretend for one minute. I can articulate the question well, but I cannot pretend to you that I can articulate the answer well at the moment.

Q13 Lord Lothian: May I touch on one other area? I have got a great deal of sympathy with what you said about the distinction between external and internal data transactions—they are getting very fuzzy at the edges and sometimes quite difficult to distinguish—but do you accept that there are reasons to have a distinction? Let me give you one example. The threshold for external data intercept is much lower than for internal. If, for instance, we are looking, which I presume we are, at what is happening in Yemen, which is, as we know, a potential source of threat to this country, is there not a justification for saying that there should be a lower threshold there—that that is a clear external and that we should be allowed, therefore, to use the same distinctions as exist at the moment?

The Deputy Prime Minister: Yes. To be very precise, on that basis I have no problem with a distinction—that a different hurdle, if you like, is set for the central mandate of GCHQ to help us to garner information from elsewhere in the world to keep ourselves safe from external threats. My concern is a slightly different one. It is that there is a risk that those lower hurdles, if you like, are applied to interactions and exchanges that, although they might be routed via servers that are located abroad, actually involve what to all intents and purposes is domestic communication. I cannot stress enough that I don't think this is wilfully happening. I don't think there is any deliberate attempt to do

it like that, but there is a clear risk, given how almost interchangeable, now, domestic communication and the external or international routing of those communications have become, that we could actually unwittingly be applying a lower—for want of a better word—burden of proof to what are, none the less, actually domestic communications. That was never the intention of the legislation, but clearly there's a technological risk, now, that that might occur, and that would make me uncomfortable, because the distinction you allude to was made precisely because it was felt that the Government of the day, the state, should have to jump over much higher hurdles when it is scrutinising legislation about fellow British citizens. I don't want to see a lower burden of proof being applied to communications between British citizens because of the technological fusion of domestic and external forms of communication.

Q14 Mr Howarth: I want to see whether you can give us a view on the warrant system—the intercept warrant. At the moment, the responsibility lies with the Secretary of State or a Secretary of State. We have heard a number of people giving evidence who have argued that that should be a judicial function, rather than a ministerial function. Do you have a view on that?

The Deputy Prime Minister: My knee-jerk response is that having a judge doing that makes sense in jurisdictions where you have a tradition of judge-led inquiries and where judges play quite a different role, candidly, from what they do in our system, where we have just a different division of labour between Executive, legislature and judiciary. So I'm not persuaded that, if you like, implanting the more activist role in the conduct of inquiries by judges, which might make sense in other jurisdictions, into ours is necessarily right, especially as long as the decisions taken by the politicians involved are properly scrutinised and held to account. That's again where—again, I know you will be familiar with this—there's real frustration on my part that if you actually read the scrutiny applied by the two commissioners, it's of a very high and exacting quality, but no one knows about it. No one has any idea about the checks and balances that are applied by way of these two commissioners. Again, I think we need to try to think more creatively about how we can bring that more into the open. There have been significant steps to do so recently, but we need to do more of that.

Q15 Mr Howarth: Do you think that that is a problem of process or resources, or is it about the culture of the judiciary, who don't worry too much about transparency? It's a question of making the right decision and you don't have to defend it—you have made the right decision.

The Deputy Prime Minister: There is a bit of a resource issue, in my personal opinion, but, again, that can be addressed. But I strongly agree with you that there is a bit of a culture there. These figures—and they are very distinguished figures—are all drawn from the senior judiciary. They do their work, they do it meticulously—they do it forensically—and they produce a report. It goes to the Prime Minister. In a sense, from their point of view, job done.

My concern, for the reasons I alluded to earlier, is that we are trying almost to re-establish or at least reinforce public legitimacy and acceptance of what the state does in secret on our behalf, and you can only do that if those forms of accountability are much more transparent, open and comprehensible to the lay observer. They are not. There is far too circular a discussion between experts, in terms that normal people do not understand.

Q16 Mr Howarth: So it is not outward-facing enough?

The Deputy Prime Minister: Yes.

Q17 Sir Menzies Campbell: Isn't the position about the commissioners really not so much about them as about the remit that they have been given? If their remit was changed in some of the ways that you have described, they would have to fulfil that remit. If we think back to the Binyam Mohamed case, which of course went in open court, there was certainly no reluctance on the part of the Master of the Rolls, for example, to express himself in terms as strong as he thought appropriate. So perhaps it is more a question of process than of substance. If you accept the job, you accept the remit and you have to fulfil that remit, so perhaps changing the remit would be enough to meet the problem.

The Deputy Prime Minister: Yes. Dare I say it, not least to you, but perhaps the candidates who fulfil this important function do not necessarily need to be limited to senior members of judiciary? I will just pose the question of perhaps opening it up to a wider field of possible candidates.

There is only one other point I would make—and we will legislate on this shortly and then establish it before the election as part of the flanking measures around the DRIPA legislation. We as a Government announced—and this was done at my initiative—that we would emulate the American model by creating a privacy and civil liberties board. That builds on the role that David Anderson has, which is obviously different from that of the commissioners but is none the less important in the whole wider architecture in which people are held to account and these decisions are scrutinised.

We will have a more established and public forum in which privacy and civil liberties concerns are tested, examined and pronounced upon when new policies are developed. That will be a helpful new innovation because it will bring out into the open quite a lot of the balancing discussions that are at the heart of this Committee's inquiry, but also often at the heart of a lot of discussions within Whitehall. Again, I hope that will bring out that iterative process of security versus liberty and trying to balance the two in a more open and grown-up fashion when new policies are developed in the future.

Q18 Sir Menzies Campbell: Could that board fulfil the function of pre-legislative scrutiny?

The Deputy Prime Minister: We are working on the details, as it happens, but the inspiration is, as I say, derived from practice in Washington, where policy ideas can be scrutinised at an early stage for their effect on privacy and civil liberties. As I am sure the Committee will appreciate more than most, institutionally within Whitehall you have, quite rightly, a strong departmental representation for security interests, but you do not have an institutionalised counterbalance that says, "Well, hang on a minute, there are also privacy and civil liberties considerations." That is what I hope the creation of the privacy and civil liberties board will do: it will institutionalise a balance in the debate at the earliest possible stage, as policy is fomented and shaped.

Q19 Fiona Mactaggart: I imagine that many Liberals would find it surprising that you are content that the Government can hold bulk data accessed in these ways, but you have been very clear about that. One thing that you were not so clear about in your speech to RUSI is whether metadata should be treated as less sensitive than content. You raised that as a question, but it was one that you did not answer. Could you perhaps answer that for us?

The Deputy Prime Minister: I do not have a neat answer. Like many of these dilemmas, all I can point out is what you can do these days. There is a semantic debate about what "metadata" really means, but let's assume for the purpose of this discussion that we use "metadata" and "comms data" interchangeably. In other words, it is about how you categorise data, rather than its content—the when and how long of a telephone call, rather than the content. Let's assume that that is what we mean by "communications data" and "metadata."

I am told that it is increasingly possible to use metadata to provide as rich a picture of what someone is up to, what they are doing and what their intentions are as it would be using content. In

exactly the same way as in the discussion we just had about there being a discrepancy in the hurdles that are set for the scrutiny of data that are held or exchanged abroad, compared with data that are held or exchanged domestically, there is also a question mark about whether there is a discrepancy on the hurdles that need to be cleared to deal with communications data compared with content. That is the founding distinction at the heart of RIPA, which is why David Anderson's review and this inquiry are so important. That legislation, a decade and a half ago, was based on a very firm view that metadata and content had completely different uses, which is clearly no longer quite as much the case as it was. That raises legitimate questions about whether we should be applying the same or adjusted hurdles.

I do not accept the first point for a minute, and I say that as a fervent, lifelong Liberal. Liberals do not slouch in saying that, in certain circumstances, the state, according to the principles of J.S. Mill, has the right to interfere with the liberties of an individual to protect society, but that needs to be done proportionately, accountably and transparently.

Q20 Fiona Mactaggart: And you think that the state holding bulk data is proportionate?

The Deputy Prime Minister: That is the question. Is it proportionate? I said earlier that I am persuaded that it is not possible to ask the agencies to do the job we have always asked them to do, which has not been the subject of debate or contention, without their having a role to do things in secret, to interrogate information or to harbour secrets to keep us safe. No one has demonstrated to me that it is possible for them to do so in this new data-rich environment in which we work without, in some shape or form, holding data inert for a temporary period of time before scrutinising an individual component within it. If there is a technological fix for that, great. I have not seen one so far. I share some sympathy with more purist critics about the state's ability to do so needing to be proved, rather than just asserted. There is a legitimate debate about whether we hem that in with new requirements, caveats, time limits and all that kind of stuff. Equally, I don't go with them as far as somehow claiming that it is an a priori abuse of the state's power to do so in the first place.

Q21 Mark Field: Picking up on one or two of the points that have already been made, I accept and agree that the zeitgeist is for transparency and accountability. However, I dare say that that level of transparency in many areas of public life has not enhanced reputation. The only exception might be the monarchy. Even then, one might argue that the move to transparency in the '70s and '80s did not do it any great favours, but it has none the less restored itself.

I wonder whether having a push towards transparency in our intelligence services would necessarily be the right way forward. There is a grown-up and intelligent mentality from the British public, which is perhaps in contrast with many other demoi, whether elsewhere in Europe or in the US, that says, "We accept that an element of their work has to be in secret and that that is the right way forward. We expect them to look after us." The quid pro quo being that they get on and do it quietly outside the public glare.

While I don't disagree that there needs to be a move towards some of the transparency that public life in the modern age demands, do you feel that there might be some mileage in having a big, consolidated piece of legislation, rather than a lot of piecemeal bits of legislation, that will allow the political class to make the case to the public about the importance of the work that is done? Should we be bringing a lot of these strands together and looking at communications data as a whole, rather than playing catch-up and updating RIPA? Rather than go through the process of having bits of emergency legislation, should we have a really good look at this issue and level with the public about what is required in the modern world?

The Deputy Prime Minister: First, of course I agree that transparency in and of itself does not magically create legitimacy. I see this issue in a much more multifaceted way. There is transparency and the publication of information. There is the need to balance institutionally, in a more

sophisticated way than is currently the case in Government, considerations of security and of privacy and civil liberties, which is why I attach real significance to the establishment in the coming months of the new privacy and civil liberties board. There is how oversight is exercised by Committees such as this. There is the role of the existing forms of scrutiny by the commissioners, and whether it is comprehensible enough and communicated enough. Finally, there is the issue of whether the founding legislative framework makes sense, given the vast technological changes.

I think we are condemned to have this great debate all over again in the early stages of the next Parliament. We deliberately created a ticking time bomb by saying that we will legislate for this, but it will lapse, come hell or high water, by the end of 2016, so the next Government and Parliament will have to revisit all this. In many ways, the Committee's inquiry, the work that RUSI is conducting and David Anderson's review all feed into what will have to be a major debate in the early stages of the next Parliament. My hope, although my experience is not encouraging in this regard, is that on this issue, if not on most others, we can seek to create some kind of cross-party consensus on the back of the recommendations of this inquiry, those of external bodies such as RUSI and the work of David Anderson and others. It would be desirable to resettle this debate.

The people who feel, for the sake of argument—I am exaggerating for effect—that the agency should be able to do exactly what it likes and should never have to explain anything to anybody will not, of course, like the move to greater accountability, balance and so on. Will we satisfy the people who feel that the holding of any data by the agency under any circumstances is a sin? No, of course not. But hopefully we can start to corral the debate in a more informed way towards a centre of gravity that strikes the right balance and is liberal—small "l" liberal, I stress—in the way in which that very considerable power and the deployment of secret authority is held to account and judged to be deployed proportionally. None the less, it must recognise that the agencies have to continue to deploy those powers, particularly in this day and age, to keep us safe.

One thing that I have learned in spades over the past four and a half years in government—this will be totally familiar to everybody in the Committee—is that conflict and warfare are increasingly becoming online phenomena. The days when it was all about tanks and battleships are long gone. We are dealing with stateless groups—we see it with ISIL—that operate in a sophisticated way online. That seems to me to be a harbinger of the future.

Chair: Thank you very much indeed. That brings our evidence session to a good conclusion. I thank you on behalf of the Committee for being so frank and comprehensive in your comments. It has given real value to the work we are doing.

17:15

The session concluded