INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

PRIVACY AND SECURITY INQUIRY

PUBLIC EVIDENCE SESSION 5

UNCORRECTED TRANSCRIPT OF EVIDENCE

Evidence given by:

The Rt. Hon. Yvette Cooper MP
Shadow Home Secretary

Wednesday 15 October 2014
(15:30 – 16:15)

Chair: I welcome you, Yvette, to this public evidence session of the Intelligence and Security Committee. It is one of seven such sessions that we are having as part of our privacy and security inquiry, and we were delighted that you offered to come and give evidence to us. We have had the benefit of your speech to Demos, in which you explained your views and the views of the Labour party. We do not have a formal programme for questioning you; we want to hear from you what you would like to share with us, but you will forgive us if occasionally we intercept to clarify, challenge or ask for further information on the points that you raise. It is meant to be as informal an occasion as possible.

Lord Lothian: Intervene rather than intercept.

Chair: Intervene rather than intercept, I am being told, given the nature of this inquiry.

Yvette Cooper: I thank the Committee for inviting me along. You will appreciate that we do not get such invitations very often in opposition, so I am grateful for the opportunity.

Q1 Chair: I want to give you an opportunity to make any general opening comments on the issues that are before us if you would like to do so. If not, we will go straight to detailed questioning. Please feel free to share with us any general thoughts.

Yvette Cooper: I want to emphasise the importance of the Committee's work and this inquiry that you are doing, and the review that the counter-terrorism reviewer David Anderson is now carrying out. We all know that in a democracy you need both privacy and security. You need security in order to be free, because you need to feel secure in order to be free, but you cannot have absolute security either. In a democracy, you also need to make sure that your freedoms are protected.

We have been very good, over many centuries, at debating that proper balance between liberty and security in the real world—in our physical lives. The debate about the balance between liberty,

security, privacy and safety online has been very limited. We had that debate around RIPA when it was first passed, but that was at a very early stage of the technology, and communications data has massively exploded since then. There have been huge changes in the way in which we all use it in our lives and the amount of information that is provided online. There have also been huge changes in the crimes that take place online—the abuse that can take place, and the ways in which it can be manipulated and used.

The police and the agencies need to keep up with changing technology but so, too, do the safeguards. It feels very much as though the pace of technology has moved considerably faster than our ability to debate the proper balance and get that balance right. Clearly, in a world where secrecy is significant, that debate is more challenging. That makes your role and your ability to ask the questions of the agencies directly, and also the reviewer's role, even more important. It raises even more pertinent questions about the strength of the safeguards that are needed.

The other thing that makes this such an important debate is that the work that the agencies and the police do to keep us all safe is immensely important, and we need them to have the confidence of the public. I think they still do have public confidence, but I do not think you can ever take it for granted. If there is a growing view that there are not the right kinds of safeguards in place, or that things are not being done properly, you cannot ever afford to see that consent undermined. That is what makes it so important to ensure that the powers and the safeguards are properly up to date, and that they are what people would expect in a democracy.

Q2 Chair: That is very helpful. Can I press you on one aspect that has interested us? The consequences of the Snowden allegations and the publicity attaching to them have given rise, in a number of areas, to heightened concern about the role of the intelligence agencies. There has, however, been quite a lot of comment about how much less that concern appears to be in the United Kingdom than it appears to be in the United States or in continental Europe. Indeed, it is perhaps relevant that most of the media did not give it the attention that one might have expected. Even in Parliament, there has been a lot of interest but not the dramatic interest that one gets in Germany and one or two other countries. Is that a distinction and, if it is, what might be the explanation for it?

Yvette Cooper: We all have our own different cultural and historical traditions. Clearly, the experience for Germany—whether through the Nazi era or through East Germany—historically is very different from ours and different again from the US experience. There is probably even a long tradition of respect for the work of the intelligence agencies that goes back to the work that Bletchley Park did during the second world war. Just because we have different historical traditions and because, historically, we have had support for the work of the agencies, it does not mean that we can ever take that support for granted. For those of us who believe in the agencies' work and believe it will be important for the future, particularly as we have changing threats, we should see it as even more responsibility on us to ensure that that consent is maintained for the future. That does mean, as expectations change, ensuring that there is appropriate transparency in certain areas, and that there are clear safeguards and clear oversight in different areas. We would take that for granted at our peril and it would not be fair on the agencies to do so.

Q3 Chair: I have one more question before I ask my colleagues to ask their own questions. From your point of view as shadow Home Secretary on behalf of the Opposition, is it fair to say that, broadly speaking, you are comfortable with the role of the agencies? You have a number of quite important, detailed recommendations for changes on oversight and a number of other issues of that kind, but is it a fair or incorrect representation to say that, broadly speaking, your view is that the agencies are deserving of public support in not just what they are supposed to do but what they are actually doing?

Yvette Cooper: We strongly support the work of the agencies. All my experience of them, as a member of the ISC many years ago and since, has been that they do immensely important work to keep us safe, but they need to have proper oversight and safeguards. Every public organisation needs to have inspection, oversight and accountability. For agencies and organisations that operate behind a veil of secrecy, the oversight and accountability needs to be even stronger. My view is that actually it is not stronger, it is weaker and more fragmented. That causes all of us problems. Even though we can support the work they do, it is because we support the work that they do that we think that the oversight needs to be stronger.

Q4 Hazel Blears: I want to explore a particular issue that is, perhaps, illustrative of some of the general points that you have made. A key part of our inquiry is to look at the capabilities that the agencies have, the way they use them and the systems of oversight around them. The most controversial issue in all the evidence sessions that we have had so far is bulk collection of data. That really goes to the heart of some of the Snowden revelations. Some of the civil liberties organisations have taken the view—they have been very honest about it—that, even if the collection and targeted analysis of bulk data resulted in targets that enabled us to prevent plots, and there was good evidence about that, they still felt that bulk collection in and of itself was such an intrusion into privacy that agencies should not have that capability. Do you think they should have that capability and, if they have it, what kind of regime should it be subject to? That seems to be at the heart of some of the controversy.

Yvette Cooper: We had quite an extensive debate about that when discussing the emergency legislation before the summer recess. It seems that there is clear evidence that holding communications data and the way it can be appropriately used has been crucial in counter-terror cases, in serious and organised crime cases, and in child abuse cases. I have a particular interest in areas where not enough is being done to deal with growing online child abuse and where more needs to be done. The examples that we had from the National Crime Agency were of cases where intelligence had been provided on those who had been involved in online paedophile networks and where it was possible for the National Crime Agency to do investigations that led to arrests in the UK. But in Germany, where they did not have the same retention of information, it led to only a handful of arrests compared with much higher numbers of arrests here. Clearly that information has been used to protect children's safety and to protect innocent people from terror threats as well. It would be irresponsible to reject the principle. The only question is how we can make sure that it is held proportionately, and that it is used in the right way with the right kind of checks and balances in place.

Q5 Sir Menzies Campbell: I want to ask you about an issue which we have already canvassed in the course of some of our evidence: the relationship with foreign Governments. You are well aware of the five eyes. Indeed, having been on the ISC, you know all about that. These are countries, putting it rather generally, with whom we have a lot in common. I don't think it is a secret that from time to time we are favoured with intelligence from, shall we say, less savoury countries. What do you think the policy of a Government should be in relation to that? In particular, do you think that in some circumstances, leaving aside the integrity of the information that is provided, it may carry a taint of how it was obtained? What sort of response do you think a Government like ours needs to have to that set of circumstances?

Yvette Cooper: We have always had strong provisions and safeguards on not wanting to deal with information that might have been gathered through torture and so on, so it is right that we should have clear principles of approach there. I will be honest and say that I find the issues involving the sharing of information across borders and with other Governments harder to assess from the outside than those which involve the domestic issues where sometimes the legal framework is less clear. The legal framework for a lot of the extraterritorial questions is harder to delve into and

therefore depends more on having access to the intelligence that you will have in the briefings you receive which I am not currently privy to. I would have a caution in answering that. Clearly you have to have a careful approach but it is an easier question for you to answer on the basis of the individual cases that you may have seen than for me to answer in the abstract.

Q6 Sir Menzies Campbell: Torture is pretty clear but what I have in mind arises out of the questions about bulk collection. If this Government—this Parliament, more correctly—took a view about bulk collection which, putting it generally, restricted it, but one was aware that information coming from elsewhere came as a result of bulk collection, would we have to pause and consider?

Yvette Cooper: There should be pause for thought. This is something the Committee should look at in some detail. It is one of the questions that we raised at the time when the information came out around the Snowden leaks. What reassurance is there that relationships with other Governments are not being used to bypass domestic legislation? Are safeguards that we might have decided as a Parliament to put in place in this country somehow being bypassed or moved around by those sorts of international agreements? That would raise considerable concern. Clearly, if other Governments have provided information about an imminent threat that they have received, then agencies will respond in one way. There is a general concern about making sure that those international arrangements do not get round safeguards that have been put in place for very good reason in order to protect the privacy of British citizens.

Chair: That was the allegation by *The Guardian* at the beginning of the process that GCHQ was using Prism and the Americans to get information. This Committee looked into that very urgently because it went to the very integrity of GCHQ. We were able to say that the law is quite clear. If GCHQ wants the Americans to help them they still have to get a warrant from the Secretary of State, regardless of whether they are collecting the information themselves or getting it from the US.

Q7 Fiona Mactaggart: In your speech in March this year, you suggested that part of the issue was public debate, leadership and transparency. We had evidence this morning from Big Brother Watch saying that the convention of never confirm, never deny, which governs such issues in Britain, must be brought to an end because it has become farcical. What is your view of that?

Yvette Cooper: The Government's response to the initial Snowden leaks was a problem. They provided so little information and response that they increased alarm rather than providing reassurance. There was very little explanation even of what the legal framework was and what the safeguards were, never mind information about how those legal safeguards might be operating. That was unhelpful.

We then had an eight or nine-month gap before we even had a response from the interception commissioner, who set out more information about the legal safeguards, but I don't think the silence was helpful. Everyone knows that of course you cannot provide full information and that there must be recognition of the need to have secrecy and safeguards in place, but it is time the Government looked again at their approach. It seemed to me at the time that it was not simply about questions about content and what was and was not happening. It was almost a case of "Let's not talk about the issues, even in principle; let's not even talk about the framework that might be in place or the sort of things that are legitimate and the sort of things that aren't." I just do not think you can sustain that in a modern democracy.

Q8 Fiona Mactaggart: But people want quite specific answers, so how far should one go in bending never confirm, never deny?

Yvette Cooper: In the end, that must be a case-by-case judgment and that is hard in Opposition without knowing the full repercussions of the disclosure of any particular piece of information and what the consequences would be. There has been a long operating assumption that the less you say about any of the agencies' work, the better, but I think we have probably moved past that now. The danger is that people suspect an awful lot of things that the agencies have never done because there are full safeguards in place. Greater transparency for the public in a series of these areas is now increasingly important.

Q9 Lord Butler: One of the things that interested me about your Demos speech was a subject you raised at the end which has not been raised much in other evidence to us. That is the exploitation of personal information for commercial purposes and your recognition that it is an international problem because the companies that do it operate on an international basis. Have you had any more thoughts about how that might be tackled, such as by means of negotiating with other countries? What method could be used to approach it?

Yvette Cooper: There are two issues. The first is the way that private companies operate with the data they have and the implications for the privacy of individuals. The second is the extraterritorial and international issues and the fact that so many companies are based abroad, even if the users are based here.

On the first issue, we have a system of cookies that most of us pay no attention to because it is a bit baffling and you are in a hurry, so you have no idea how much data is held by private companies. They do not use it to solve crimes or to prevent terrorist attacks. They use it to make money. They make money on the basis of our information and our data. Much of that may be perfectly legitimate and it may mean that we can get access to free websites because we also put up with targeted advertising. The advertising from whatever website we have previously shopped on suddenly pops up when we go on to a news website. That may give us free access to the news websites. However, the assumption that private companies can do anything with our data without that ever being challenged or debated will become an increasing problem. People will increasingly feel that their own data should be something that they should have more say over. I do not have easy solutions to this because there are much wider economic questions, as well as the technological questions, with the way in which it works. I simply raise it as something that I think will become an increasing debate about our privacy in an online age. It is a private sector question, not simply a Government and public sector question. Sometimes the edges will overlap and sometimes they won't, but we should not ignore the private sector privacy issues as well.

On the second part of your question, which was about the international jurisdiction, one of the sections of the emergency powers Bill before the recess included extraterritorial provisions. This is a very difficult area of law as well as a difficult area of the technology. Some of the domestic debates that we have about this feel like they are going to be completely overtaken by some of the wider, international consequences. One of the reasons we were very keen for the RIPA review to take place was to look in more detail at some of those extraterritoriality issues. The provisions that the Government had in the draft Communications Data Bill, which now seems to have stalled—we have never seen the revised draft—did not feel like a very satisfactory attempt to solve the international challenges. That may be something that will require far more co-operation between countries. The work that the Government are now doing on the MLATs approach is extremely important, but I am not up to date on how much progress they have managed to make with it.

Q10 Lord Lothian: You were talking about transparency and I think we all totally agree with that. The real problem I have with this is that if something is going to be transparent it has to be understandable. If you look at RIPA, somebody said you have to read it with a lawyer beside you to understand it.

Another area that goes to the whole question of transparency is understanding the difference between domestic intercept and overseas or external intercept. The question is about where the message begins and ends. I thought, about three months ago, that I understood this until suddenly I start reading about cloud. I wonder whether anything sent to cloud, whether from here or anywhere else, is actually external because cloud is based somewhere in California. All of those areas make it very difficult, in my mind, to be transparent. Have you got any suggestions for making all this much simpler so that the public can begin to understand it? Out of that transparency we might get more trust than we have at the moment.

Yvette Cooper: I know, and I fear our children may understand it rather better than we do. There are two things that make it hard; the legal complexities and the technological complexities. It was a problem that the Government did not translate RIPA at the time when a lot of the concerns were being raised and that they did not explain what the current framework does. There are areas where I still think it is hard, even having spent a lot of time looking at it, to be clear what certain sections do and do not provide for. It also shows that with the pace of technology, it is now out of date.

There are a series of areas; one is the internal/external, the difference between domestic and foreign. Quite understandably and quite rightly we have had stronger safeguards around domestic communications over a long period of time. We have also had stronger safeguards around intercept, compared to communications data. However, those distinctions now seem to be much more blurred and difficult to sustain. I agree with you on the internal/external one. When communications travel all around the world and back again between two people in the same country, that clearly raises questions about the way in which the existing framework operates, the way in which data is gathered and how far it is possible to gather information simply around foreign communications or simply around domestic communications.

The other area is this distinction between communications and content. To me, that does not feel like a clear binary distinction at all anymore. An interesting example—I referred to it when I was doing a speech—was that of Churchill having an argument with the post office in 1911 about whether he could open letters. That was a debate about content. It was about whether the police were able to look at the letters being sent between two people. Even then, they would be able to look only at what was in the letter and the communications between two people at that time.

With communications, which are supposedly less invasive than the content of that letter, you can find out not only who people have been contacting and who all their friends are on social media websites, but where they shop. Weblogs are categorised as communications rather than content. Some people argue that video shots of live chats are regarded as communications rather than content. A whole series of things can tell you an awful lot more about a person than that one letter that someone might have sent in 1911.

In such circumstances, do we therefore need to look again at the safeguards that are in place for different levels of surveillance and investigation? I think we do. The Joint Committee that looked at the Communications Data Bill made a very strong case for looking again at different kinds of safeguards, and stronger safeguards for different aspects of data that are currently regarded as communications data. I think the relationship between communications data and content data needs to be looked at again, and obviously we will have your reflections on that, and also David Anderson's, as part of the RIPA review as well.

Q11 Mr Howarth: Can I change the subject to oversight, particularly how the oversight works in these sorts of cases? It starts with a Minister authorising through a warrant. That is the audit, and the follow-up on that is through the commissioner. Finally, if there is a complaint, it is through the tribunal. Do you think that that is the right combination of checks and balances? If you do, do you want to say a word about its being perhaps more transparent so that people understand the system better and know who is doing what?

Yvette Cooper: The oversight needs to be stronger. If you have strong powers in place, you also need strong checks and balances. They need to be stronger for agencies that inevitably need to operate behind closed doors. There clearly needs to be a process of warranting in advance, but also further checks and safeguards on what happens afterwards and along the way. I would argue for oversight to be strengthened in a series of different areas. I do not think the commissioner system works very well. It is too inward looking, it is not flexible and fast moving enough, and it still feels too much as though it is operating as part of the Executive, rather than being an independent check.

Clearly, there has to be a process of checking legal compliance with warrants, but there also needs to be a wider way of being able to have investigation, oversight and inspection into the way in which the agencies operate, and we need to know whether the existing legal framework is still up to date, for example.

The commissioners will often say that their role is simply to check compliance with existing legislation. If the existing legislation is not up to date any more and has been completely surpassed by the pace of technology, who will provide enough investigation and enough detailed scrutiny of what the agencies do to be able to recommend amendments in future? It does not feel as though the commissioners are currently able to do that. They are also not outward facing enough. They rarely do media interviews. They see their role very much as providing—this is how it is set up in the legislation—information and reassurance to the Prime Minister that things are happening in the right way and that legal compliance is there, whereas in a modern democracy you need the public-facing accountability.

The role of the counter-terrorism reviewer is a much better one. That seems to work much more effectively. The fact that David Anderson will do interviews, talk to journalists and the agencies, and has managed to get the respect of civil liberties campaigners and the agencies is quite important. He is also responsive enough that if new problems and issues emerge, he can say, "I will look into that." The commissioners rarely do that. I welcome Paul Kennedy saying that he will look into the use of RIPA with journalists' sources, but he has not said very much publicly; he simply issued a statement. Having that kind of public-facing approach would be important.

The police and the Prison Service do not simply have a committee to provide oversight; they also have inspectorates. HMIC looks into the police, and the prisons inspectorate looks into prisons. There are formal inspectorates looking into them. For the agencies, we have narrowly defined commissioners looking into very judicial aspects, and we also have the Intelligence and Security Committee. It feels to me as if that provides considerably less oversight than we have for other agencies, even though there is arguably a need for greater oversight behind the veil of secrecy because those agencies inevitably do not have the same media scrutiny and public scrutiny. That is not there at the moment.

Q12 Mr Howarth: Several witnesses have suggested that the signing of warrants should pass from Ministers and become a judicial process. Is that a way forward or might it be problematic?

Yvette Cooper: I am open-minded about the intercept warrants. In other countries where there is judicial oversight, it is not necessarily clear that judicial oversight provides greater scrutiny. It being judicial rather than Executive clearly provides some level of independence. There is no reason to believe that the Secretaries of State who have to sign the warrants do not provide very considerable scrutiny and will very much think of the consequences if they get things wrong. I am still open-minded about that. You could do things through a judicial or a ministerial route in terms of signing the warrants. The current framework, in which a Secretary of State has to do it, limits the number on the basis that they are able to spend a certain amount of time going through the warrants. You might not have that in a judicial system.

Q13 Mark Field: I want to touch on plans for legislation. I appreciate that you have an election to get through before and—who knows?—there might be a coalition, which has been one of the constraints on getting legislation through. You are right to identify that there is still a broad sense of trust in our intelligence services, elements of which are historical. We saw with *The Guardian*'s Snowden revelations that, beyond a relatively small group, there is a sense among the public at large of, "Actually, that's what we expect our secret services to do—to be secret, get on and do their bit to protect us." However, I think there is a lot less trust for the police and a lot less trust, I am afraid, for politicians and the political process. Do you have any sense that, in an ideal world, you would like to have a broader, consolidating bit of legislation here, to be able to make a case, both as a Minister and within a Government, for the importance of our intelligence services, to try to sweep up a lot of this? There is a sense that the legislation—RIPA—is not any longer entirely fit for purpose, 14 years on, but ever more piecemeal legislation may not be the right way forward. A much bigger consolidation may bring much of the political class forward to be broadly supportive of what is trying to be achieved.

Yvette Cooper: Until we have seen the conclusions of the RIPA review, it is hard to answer that question fully. My assumption has been that we will need a replacement for the RIPA, but we will obviously have to wait until we have David Anderson's recommendations about whether that can be done through amendment, or whether you need a new framework in place.

There is a problem with the debate around the Communications Data Bill, which was obviously the Government's attempt to do some more about this. We always thought that it was far too widely drawn. The Joint Committee's report was sensible in pointing out the problems with that. I understand that there is a second draft of that Bill, but I have never seen it—we have never looked at it—so, again, it is hard to know what proposals it contains and how that will relate to the RIPA review as well.

I think that, clearly, new legislation will be needed, if only to deal with some of the issues around communications and content, the additional safeguards that are needed, and the stronger oversight that I think is needed, but quite how broad that will need to be will depend on the RIPA review.

It occurs to me—we will obviously be interrupted by the bell—that one thing that should be looked at is whether all the commissioners should be brought into a single stronger framework for oversight, rather than the fragmented system: a sort of single inspectorate. Looking at the models in other countries, some have tried this but it has not worked and some have tried it and it has worked. A single inspectorate is the sort of thing that we should be looking at.

Q14 Mark Field: And you envisage this being a fairly urgent bit in your in-tray, if you were in a position to be Home Secretary come next May or June. Would you see this as something that would be dealt with within a—

Yvette Cooper: Yes, I think it is needed, because the emergency legislation that we passed before the recess is obviously time-limited, so, clearly, those elements in terms of retention of communications data will need to be addressed again, and it is right to have the stronger safeguards in place as part of dealing with that. That was sticking plaster legislation that we did before the summer recess. We should not do repeated sticking plaster legislation; we should try to do it properly, in some detail.

However, that means that you need to have a public debate, so the opportunity needs to be there. Once we have David Anderson's conclusions, there should not simply be a rush the next day into legislation that the Government have prepared earlier; we should have the proper debate on those conclusions and then move to legislation.

Q15 Dr Lewis: Every one of the witnesses whom we have seen so far has been happy to acknowledge that particular surveillance of individuals who can reasonably be suspected of planning to do harm is perfectly acceptable, even though it involves a compromising of their normal qualified privacy rights. However, as Hazel said right at the beginning, under sustained questioning from the Chairman, most of the civil liberties groups, and some academics, but not all of them, said that even if a major attack could be prevented by bulk data gathering, they would still say that bulk data should not be gathered and that the price of the attack was worth paying. I should like a little bit more of your view on that approach.

One option that some of the academics put forward in relation to that was to say, "Well, it would be better, if we have to do bulk data gathering, that that bulk data should be held by the private companies that gather it, rather than by the state." However, the Parliamentary Office of Science and Technology did a survey for us on public attitudes to personal data and privacy and concluded that, generally, people report that they trust Governments' intentions more than commercial companies' on data security and protection from data misuse and fraud. Indeed, 57% of people support Government monitoring e-mail and internet search traffic to identify potential terrorists and people with extremist views, although 25% oppose this.

Putting that basket of things together, do you feel that, on the whole, if bulk data is to be retained, we should go down the route of private companies retaining it or of the state doing so?

Yvette Cooper: The arrangement we have at the moment is that communications data are held by private companies. I think that is considerably preferable to its being held in any public sector form. It is interesting that it is the route that President Obama has chosen to move towards now, having previously had a system where it was held by arms of the state; that is now shifting, to trying to have those data being held by the individual private companies instead.

Having a system where those companies hold the information and the police or the agencies have to put in a request through a proper warranted process just provides additional safeguards. Clearly, there will also have to be safeguards on the way that those private companies hold the information and there will need to time limits on its being held, and the way it is used has to be proportionate. So you must have strong enough safeguards in place and it is right to keep those safeguards under review.

There is an interesting thought about who, in the end, people trust. I remember people pointing out evidence that showed that the public—I think this was true in both Australia and Britain—were strongly in favour of identity cards until the Government proposed them. As long as they were being proposed by everybody else, including private companies and private organisations, everybody thought they were a great idea. As soon as Governments and politicians start proposing them, people become rather less keen.

So I would have that as a caution in respect of what people's attitudes would be about whether this information was being held by a public sector or private sector one.

Q16 Hazel Blears: Your grasp of the issues is hugely impressive, and these are not simple matters.

Sometimes I am disappointed that parliamentary colleagues do not perhaps take quite as much interest in the kind of oversight that we endeavour to do. Traditionally, we have had an annual report and an annual debate, which tends to be a debate among ourselves, rather than necessarily being held more widely among parliamentarians.

I wonder whether you have any ideas about how we might engage Parliament a bit more in the kind of oversight and scrutiny, through debates, and whether one way we might do that is by subjecting Ministers to greater scrutiny in the House for some of the decisions that are made.

It is quite disappointing that, unless there is a crisis, like the Snowden revelations, or something comes up, on a day-to-day level few colleagues are engaged with important matters of national security.

Yvette Cooper: That is right. It is a challenging one. In some ways, I suppose the question is also whether it is possible to engage the public more in the debate, which then makes it more significant in Parliament. When Parliament has engaged with such matters it has often been because MPs were being contacted by constituents about them. If they get letters and e-mails about this, rather than about some other issue of concern, then that will make people more likely to look into the detail of it and to become involved in the debates. So that is probably one way of doing so.

I think you are right: it is important for Ministers to be more transparent about what the issues and crunch questions are.

The question for us over the next 12 months is probably how the conclusions of your report are aired and properly debated, and then how the conclusions of David Anderson's report are, too—and that there is opportunity for detailed consideration of those reports and for as many people as possible to be involved. That goes back to the questions at the beginning. If you do not have consent, it is much harder for any of the security work that we need to be done, and for anybody to have confidence, both that their privacy is being protected and that, unless they are suspected of some terrible crime, their e-mails and data are not going to be investigated in any way and, at the same time, be confident that the agencies will be doing what is needed to keep people safe. But that all depends on the framework of consent, and that depends on there being a level of knowledge and understanding as well.

Q17 Chair: A final question, if I may. Since the 1990s, the intelligence agencies, to a considerable degree, have come out of the shadows and are much more public in terms of their leadership and their speeches, and so forth. It is sometimes said that the agencies have been more willing to do that than various Home Secretaries and Prime Ministers have been willing to allow them, and that there has been more reluctance on the part of Government.

It is easy, as shadow Home Secretary, as opposed to Home Secretary, to say, "Yes, I believe in more transparency and more openness", but do you think, as Home Secretary, you would be able to, and would wish to, implement reforms in that direction?

Yvette Cooper: I think you have to. I think that if we try to keep everything behind closed doors, the danger is that we will undermine the trust that we need for the agencies to be able to do their work. So I think, in the end, it is damaging to confidence in the agencies to try to keep everything too quite and too silent. You need to build that confidence.

You are right. Of course, that is something people often say more in Opposition than in Government. However, if you believe in the work that the agencies do, making sure that they are able to demonstrate to people that the safeguards are in place and that the work they do is important, really matters, and it will probably matter even more in future, as you have growing technology as well as ever more complex threats that need to be dealt with, and changing public attitudes at the same time. We are, as a nation, going to have to be increasingly nimble about keeping up with those debates, and we are going to need to adapt, whether to changing technology, changing expectations or changing threats. You cannot adapt unless you have consent and consensus about the principles that should guide us and on the way in which we should respond.

Chair: I thank you on behalf of the Committee for your valuable contribution to our work. Hazel mentioned that you were extremely well informed and clearly in command of your brief. I think we would like to believe that that must be because of the years you spent as a member of the Intelligence and Security Committee.

Yvette Cooper: It must be.

Chair: Perhaps that should be a condition for future tenure in the office of Home Secretary. Thank you very much indeed.

Yvette Cooper: Good luck with your report.

Chair: Thank you.

16:30

The session concluded