

WEDNESDAY 14 NOVEMBER 2007

Present

Bledisloe, V
Goodlad, L
Holme of Cheltenham, L (Chairman)
Lyell Markyate, L
Morris of Aberavon, L
O'Cathain, B
Quin, B
Smith of Clifton, L
Windlesham, L
Woolf, L

Rodgers of Quarry Bank, L

Witness: **Mr Richard Thomas**, Information Commissioner, **Mr David Smith**, Deputy Commissioner and **Mr Jonathan Bamford**, Assistant Commissioner, examined.

Q1 Chairman: Mr Thomas, welcome. We are very glad to see you here. Would you be kind enough to identify your colleagues?

Mr Thomas: Thank you, my Lord. On my right is David Smith, who is my Deputy Information Commissioner and on my left is Jonathan Bamford, who is the Assistant Commissioner with particular responsibilities in this area.

Q2 Chairman: Your appearance before us is really the first substantive evidence we have had in the new inquiry on which we are embarking, and we are delighted to have you here. In fact I can say that your own writing and speaking about the surveillance society has been part of the inspiration for our work. Is there something by way of an opening statement that you would like to say to us?

Mr Thomas: Thank you very much, my Lord. We are delighted to be here this morning. We are very pleased that this Committee has launched this inquiry. We have submitted written

evidence to the Committee and I hope that this morning we can highlight and elaborate some of the points in our written submission to the Committee. I think you are aware of – and we have provided to you – the report that we published this time last year, November 2006, which we commissioned from the Surveillance Studies Network for a conference we held in London, and that elaborated the situation as it was in 2006 and also rolled forward to what life might look like in the year 2016. The nature and the extent of surveillance involving the collection and processing of vast amounts of information about our private lives does raise some fundamental constitutional issues about the nature of society, about liberties, freedoms and human rights, about the autonomy of citizens, about the role of the state and about the relationship between state and citizen. Surveillance is perhaps traditionally associated with totalitarian regimes but some of the risks can arise within a more democratic framework. Our role has been primarily to raise awareness and stimulate debate. We wholeheartedly welcome the focus which this inquiry will bring on the issues and I think it is part of a general raising of awareness which has been going on perhaps over the last 12 months, about which we are very pleased, because before then there had been a quite substantial lack of awareness and a corresponding lack of public debate about many technological, governmental, policing and commercial developments. We think there is need for much greater attention to be focused on the risks involved and the safeguards which are needed. We all now leave our electronic footprints in many places on a daily basis and as the pace accelerates our concern is to ensure that full consideration is given to the impact on individuals and society, that pre-emptive action is taken where necessary to minimise intrusion, and that measures are in place to safeguard against unacceptable consequences. The issues certainly, we think, are complex and controversial – there are no black and white or easy solutions – but we think that the more debate and discussion before some developments become irreversible, before the risks materialise and before there is a public backlash is very important. We are very keen to

emphasise that certainly we are not suggesting that any sort of surveillance society is developing for malign reasons; it is more the cumulative effect of separate developments with benign and well-intentioned purposes. We believe that the report we published last year served as a wake-up call on the various dangers that can arise in this area. We believe that there are risks and there are dangers which can result from excessive surveillance, and this can be divided very broadly into those which impact negatively and sometimes very seriously on individuals and those affecting society as a whole. Both types of detriment can arise from mistakes, from inaccurate or outdated information, from security breaches, from excessive intrusion, from the hidden collection of information and from the unacceptable use of information. The risks grow as ever increasing reliance is placed on single or centralised collections of personal information. We are very pleased, Chairman, that the debate has now broadened; there are not many subjects where the *Daily Mail* and the *Guardian* can both unite on these sorts of issues with the coverage they have been giving to them over the last year, but also there have been some very thoughtful articles quite recently, for example, in *The Economist* and in *The Sunday Times*, which have given a very full analysis of the various issues, and we are pleased to see that level of debate going on.

Q3 Chairman: Thank you very much. You have touched on a number of the issues which will concern the Committee, but can I start by saying something that has come very clearly to our attention, even in these very early days of deliberation, which is the difficulty of getting any 360 degree review of these issues. Even in the evidence given to us by the Ministry of Justice we find the lack of any overarching 360 degree context; there seems to be no general principles nor a firm legal basis, nor a whole-of-government view across departments, or for that matter an overarching regulatory framework. We are dealing with an area growing like Topsy – very fast – and driven by change, both social and technological change, and I think one of the problems that the Committee has already had is to try and get our mind around it as

a whole, and I would be grateful before we get into some of the detailed questions if you could give your reaction to the partial and sporadic growth of public policy and law in this area and what your reaction is?

Mr Thomas: I think, Chairman, we would very much agree with that sort of analysis. I think it is fair to say that there has not been a single point of reference for all these various developments. The work that we have done has ranged widely; it has drawn attention to very many fragmented developments across both public and private sectors and within government where virtually every government department is involved in one way or another in issues which impact on this subject matter. The Ministry of Justice is a focal point for data protection but the Home Office, the Department for Transport, the Department for Children and Schools, the Department of Health, all in their various ways have an interest and are doing work which has a bearing on the issues with which we are concerned. I think there are signs of a sea change; I think the Prime Minister's speech on Liberty on 25 October, which devoted some five pages to looking at privacy and data protection issues, was the first time I think in living memory that a Prime Minister has addressed these issues so fully and already there are signs that that is sending out signals across Whitehall that the protections and safeguards must be taken very much more seriously. Over recent years perhaps there has been a push to gather more and more information, to harness the benefits of technology without perhaps giving thought both at the fragmented level and at the general level as to some of the implications, some of the safeguards needed. Your final point perhaps was about the regulatory framework. I think we would say that the Data Protection Act, the legislation on the data protection, does provide a broad, horizontal framework and although I and others have some reservations about some of the detail of the legislation, the fundamental principles which lie at the heart of this in the European Directive and at the heart of the 1998 UK Act I think have broadly stood the test of time. I think they do address the sort of safeguards that we

need to have in place and we can elaborate this morning as to how we are trying to apply those in practice. So I think the principles are sound and I think they do provide a good reference point for judging what is acceptable and what is not acceptable, but perhaps some of the machinery for implementing that is getting a bit creaky now and we might look at ways to improve that.

Q4 Chairman: I am sure we will come back to that in the course of the questioning. One thing that the Committee has become aware of in preparing for this inquiry is what is called profiling, where a set of people in society are created through shared data characteristics which then potentially determines public or penal or other policy towards them. Since a lot of the emphasis is on the individual I wondered whether you could talk about the indications of profiling as a guide to policy approaches in a number of areas and any dangers of which you are aware.

Mr Thomas: Perhaps I could start on that and then ask one of my colleagues to take the issue a bit further. Perhaps in some way the starting point is what has happened in the private sector. Everybody in this room will be aware now of how sophisticated marketing has become in recent years – holiday companies know where you are likely to want to go on holiday, Amazon will know your reading habits. The private sector has become very sophisticated, using a lot of commercial information, postcode information and so on to really build up a picture about our preferences and our experiences. I think the public sector is, if you like, catching up in this area. The police are enthusiastic about profiling and one can see perfectly legitimate uses of profiling when they are trying to deal with particular types of criminal behaviour and I do not think anybody would have any difficulty with that where it is done properly. Likewise, profiling is now being talked about more and more in the area of child welfare, child protection, in the health area and so on. In principle targeting people so that we know what the issues are in the public sector, with which we are dealing, is a good

thing and we are keen to emphasise that. But there are dangers. I can give you one example: we know that some 20 per cent of adults commit 80 per cent of crimes but does that justify looking at children as they are growing up, looking at the criminal records of their parents, looking at the social circumstances of their household to say, “That is a likely criminal for the future who needs particular watching in the classroom or in the local community”. An even more acute example is that there is evidence to correlate the link between victims of child and sexual abuse and those who later in life become sexual abusers themselves. Does that justify taking a profile of victims of sexual abuse and saying, “We have to watch these people very closely because they may be the offenders of the future?” There are other examples which my colleague might share with the Committee.

Mr Bamford: Building on what the Commissioner has said, we see many aspects of risk assessment in administrative life. When you have stretched resources, when you have particular problems you focus on risk and look for risk areas, and that is the area where profiling comes into its own really; it is trying to use information to direct your resources and your interests into particular areas. I tend to use the example of the children who are going to grow up to be the 20 per cent of adults who commit 80 per cent of the crime then we end up with the situation of that activity generating lots and lots of information. So you see that there is more and more information being utilised to try and tease out these risk factors. When you are working with a degree of certainty maybe that is not a bad approach but when you start to deal with some more nebulous matters that becomes a bit more difficult, so the criteria to generate the risk is flawed in some way. So we see dealing with risk generates profiling; we see it in the public sector and we see it in the private sector. You could say it may be more in the private sector for profiling customers for good things; in the public sector we often see it for things which have a detrimental effect on individuals – whether a person should be

allowed on to an aircraft or not because they happen to share some characteristics with somebody deemed as a risk.

Mr Thomas: I think there is a wider debate and this is covered very fully in the report that we have published, that the more you use profiling the more you run the risk of going down a society where there is greater stigmatisation, more discrimination, more social exclusion and a society of greater suspicion where trust is reduced.

Chairman: Where the data becomes predictive, if I can extend the example you both hinted at, I think I am right in saying that if you are a special needs child in a school you have about a three times higher probability of being excluded from school than the average child. Then we learn that children excluded from school have about a three times greater likelihood of subsequently becoming offenders. So it is quite a skip and a jump from a child having special needs at school to saying that such a child has a nine times higher probability of offending than the average child, and it then becomes a predictor of policy. I think Baroness Quin has a question.

Baroness Quin: It is certainly an area about which I am concerned as well in terms of the fact that it might blight someone's chances of employment and getting opportunities in life afterwards, and I wondered if you felt that there was a bit of a problem between the need to try and protect society from risk and yet the principle of believing in rehabilitation? If someone has served a sentence then they have paid their dues to society and should not be penalised for the rest of their lives.

Chairman: I am going to take Lord Bledisloe who has a question on this point as well.

Q5 Viscount Bledisloe: Taking, for example, these children that you refer to in your paragraph 7, the ones whose fathers were thought to be regular burglars or, indeed, the ones who are thought to have been victims of abuse, surely at the very minimum they must be told that they are on a register because of that because they may want to say either, "He was not

my father,” or “But he moved out of home when I was one and had nothing to do with me”, or he may want to say, “You have got it wrong.”

Mr Smith: There is a very good example, Chairman, both of stigmatising and of competing public policy objectives in the checks that are made on people who want to work with children, particularly criminal records checks; and it goes more than into the criminal record, it is actually that any information held by the police can come out in a check. We had a system which was inadequate; it allowed people to work with children who were not subject to proper checks. But in addressing that public policy concern we have gone very much the other way, so that if I applied now for a job to work with children any conviction that I have ever had would be revealed to my potential employers, whether or not it had any bearing at all on my risk to children. So the fact that I was convicted of shoplifting as a teenager, which was unfortunate and I regret it and I have put it behind me, will come out. If that employer refuses me the job I will think it is was because of that conviction whether it is the case or it is not. I will think that I have been prejudiced against. I have no doubt that in the risk averse climate we have with child protection with any speck that is there employers will say, “No, we will leave that person alone, we will go for someone else.” So I think that is a very good example. The other example, which is slightly different, is to do with airlines and airline passengers where there is a profiling arrangement – people present risk factors. One of the problems that you see, particularly when people go to the States, is that the same people keep getting stopped. They may present under the profile at one time, they get stopped, they get questioned, but then there is not the information management processes to update the profile so the next time the record says, “No, this person may present but do not stop them.” It is about proper information management processes to go alongside the increased collection and use of information.

Q6 Chairman: I think the links you have all made between over-zealous risk management and surveillance is a very important one. Thank you for that. Can I move on and ask you, in terms of the plethora of current and proposed policy initiatives with which we are faced, are there any that you as Information Commissioner see as posing a particular threat either to the privacy of the individual or the well being of society?

Mr Thomas: Perhaps I could give you a list of current initiatives which I think have a bearing on this and we can develop that? I think the identity card debate and the national identity register, the database behind that is an area that has been of particular concern to us. The e-borders programme; Connecting for Health, the National Health Service project to have full electronic health records in due course on every person in this country; the road user charging possibility if we have intrusive means of tracking vehicles as they are driving around the country; the Serious Crime Act which has just very recently received Royal Assent is an example of authorising public sector access to private sector databases in the fight against fraud; the new rules recently brought forward for the retention of telecoms details by telephone companies with access to that by the police. Those are just some examples and we can say more about any of those as you choose.

Q7 Chairman: All of those, their proponents will claim, have social and other benefits. Of the ones you have identified – and it is a very helpful list – are there any where to you, as the Information Commissioner, the negatives clearly outweigh the positives?

Mr Thomas: We are very conscious that we are appointees; we are not a democratic institution, and so when Parliament decides that there should be an identity card system we respect the will of Parliament on that. At the same time we are aware of the controversy as that was going through Parliament. We engage with the Passport and Identity Agency, and indeed we have a meeting this afternoon to look for how that is going to work in practice, to try and minimise the risks to citizens. We have always made it clear that one of our major

concerns has been the database – it is not so much the cards it is the database behind the cards – and we continue to question why so much transaction data is going to be collected. It is one thing to have a card to prove your identity but why do we have to have a record on that database every time the card is swiped through a terminal, whether at Heathrow, at a police station, at a social security office or wherever? We have questions about the database of all children that is being put together in this country, every child from birth until 18 years old. We can fully understand the rationale for collecting information about children who are at risk of physical or mental abuse or other forms of unacceptable treatment from their parents or their guardians; no one, I think, would quarrel with the need for social services, the police, and the schools to at least be aware of the children who are at particular risk. But we are more sceptical about the need to keep even basic information on all children with the rather more vague purpose of safeguarding their educational development, their health and their social circumstances. I think that is an example where we still have some reservations about a particular database.

Q8 Lord Goodlad: Commissioner, you mentioned the Prime Minister's recent speech on Liberty in which he mentioned the importance of parliamentary scrutiny of legislation and the granting of powers involving the collection and use of personal data. It would be of great interest to the Committee if you could say how well, in your view, Parliament has been fulfilling this role and what, if anything, you think could be done to increase the effectiveness of parliamentary scrutiny?

Mr Thomas: Thank you, Lord Goodlad. I have mentioned the Prime Minister's speech and I am certainly not making a party point. I thought it was a thoughtful speech on the subject of liberties and I thought there were some very welcome words there about recognising the need for balance in this area. The Prime Minister talks about the need for security against terrorism, the fight against serious crime and fraud; he talks about the improvement of public

services. He recognises the benefits of collecting information but he is also very, very clear about the risks. He talks about accountability where people's data is concerned and that government needs to be held, he said, independently to account and that we risk losing people's trust, which is fundamental on all these issues. So I very much welcome what was said in that speech. In terms of parliamentary scrutiny I think it is hugely important that Parliament is vigilant, if I can be so bold, to scrutinise measures as they come forward, and perhaps there has not always been as much scrutiny as I would like to see. In 2003 the legislation was changed to allow the expansion of the national DNA database and that now allows DNA to be retained indefinitely on anybody who is coming to the attention of the police because of any recordable offence, even though they are not prosecuted. Even though they are not convicted the general rule now is that the DNA profile is retained indefinitely. There was not very much debate about that in Parliament. I fully recognise that technology has moved on and perhaps when that was being debated it was quite expensive to obtain DNA profiles. But now technology, even in the last five years or so, has made it much easier to obtain and retain DNA. We are now in the situation where I think probably there are more DNA profiles on the national database than anybody would have contemplated when that was going through. So I think the more the better that Parliament is looking both at primary legislation, which creates the framework, but also at the detail of the secondary legislation – often the devil can be in the detail. I have mentioned our meeting this afternoon where we are going to be discussing the secondary legislation associated with the Identity Card Act and I think it is important there should be as much debate as possible – certainly in Parliament but elsewhere as well, and I am sure that Parliament would not claim any sort of monopoly of scrutiny, and we ourselves have a very important role in trying to alert people to some of the issues. There have been occasions where the parliamentary process has improved the quality of legislation. The Serious Crime Act, which received Royal Assent, was significantly

improved on a cross-party basis as the Bill was going through the House of Lords. The new provisions there, which were taken as amendments, were modified slightly in the House of Commons, which essentially say that there should now be a statutory code of practice to govern the public sector access to private sector databases; that there should be a code of practice which should be put together in consultation with myself and that I, as part of that code, should have the right to go and inspect how these arrangements are working in practice. It is not just the codes and the fine words in the codes; it is how they are working in practice. Although we do not have a right under the statute, which I hope we might come on to later – we have no legal right – we now have, if you like, in that particular example, as a result of the parliamentary intervention a quasi contractual right under the code of practice that we can go in to inspect. That is a very good example of Parliament increasing the safeguards in place.

Mr Smith: Could I perhaps put in there a plug for our position because we have a power to report to Parliament, which we have used very occasionally – and we will refer to that later – but where Bills are subject to parliamentary scrutiny we are very happy to come and give evidence to the relevant parliamentary committees, and we do that. But it is rather haphazard as to whether we get invited, whether there is investigation of our areas. We wonder whether there is some scope to formalise that arrangement whereby we have a right to be heard or something of that sort in the process where there are significant implications in legislation for the use and collection of personal information.

Q9 Chairman: It is possible that Parliament would like to find some way of knowing on an Information Commission radar that *prima facie* you think this raises an information issue that might be worth thinking about.

Mr Thomas: We are not seeking to expand our empire, Chairman, I assure you, but equally our counterparts in other countries do have that sort of function and we think that perhaps the time has come for a little more formalisation of that. It is not just the parliamentary stage, I

think we all know that it is at the early stages of policy development and on some occasions government departments have moved forward two or three years without involving us and by that time things get rather set in concrete and it is too late to go back several stages.

Q10 Lord Morris of Aberavon: Questions were asked in the House of Lords regarding the extension of DNA and I do not think we pinpointed sufficiently the fact that there would be millions and millions – and in due course possibly all of us – on this register. In the old days fingerprints of an accused person, if acquitted, were destroyed. Now “coming to the attention of the police” were the words that you used, everyone is going to remain on this. Did you at the time say anything? Should you have said something? I think I gather from what you have just said that there should be machinery for you to say something to express any concern that you might have?

Mr Thomas: I started at the beginning of 2003 and perhaps we missed a trick in not shouting loud enough. I think we did put in a paper on the subject but perhaps it was not very well publicised and perhaps did not really have the force that it might have had, so I think we recognise, moving forward, that we need to put our views as forcefully as possible. But these are difficult issues. On the DNA database we fully recognise its functions – there has been a case this week where a conviction has been secured many, many years after the event and I think everybody would welcome that. But we would question, for example, if, as a citizen who does not have a conviction and your sample is taken and it is run against the database of samples taken at scenes of crime, if you are clear – why does that sample have to be kept indefinitely? It is one thing to take a sample and apply it on the spot, as it were – maybe it takes seven days – but why should that be kept on an indefinite basis? What we are also saying, going back to the Chairman’s opening comment, is that there are so many developments across so many aspects of public life now that I think we could not undertake to get involved in every single one; what we would like to do is to have a stronger right to come

forward – either the law requires some consultation with our office or that there is a duty when a new scheme is being introduced to consult with us. I would like to say more later about privacy impact assessments because I think that is a technique for addressing some of the issues as schemes come forward, but I think there are various techniques to give us a more formal involvement.

Q11 Baroness O’Cathain: I am going to take a rather different view actually. I feel rather comforted by a lot of the information that is collected on me and I also believe that longer term having the DNA of everybody in this country might not be a bad idea because there are huge benefits in having it, at least those people who are most likely to commit crime. I think we are terrified of this whole criminal side of it. A very simple example of the positive benefit of data collection, which I made when we were talking about this. When you go to license your car you can actually do it in two minutes and not take your MOT and not take your registration book and not do anything else. I have to tell you that that is a great advantage as all data is shared between DVLA and the Department for Transport. Secondly, if you are involved in an accident and if, for example, your DNA was on a register they might say, “This is a person ...” - and because relevant health data is stored – “... for goodness sake do not give them penicillin otherwise they will be really dead.” I feel that the more information that is held centrally on me the more I am comforted, and secure. But that of course then raises the question of what hands does it get into? But before we get to the point – and I would like your view on this – you made the point that everybody knows so much about us – and again we have spoken about the Tesco syndrome where they literally will not give you special offers on alcohol if they know perfectly well that you never drink because you never buy your alcohol there. They have literally built up a profile on you – it does mean that you get a lot less junk mail. The third point is that we still have – and is this going to continue – a situation where if you subscribe to magazines they ask you your profile or if you

do something like buying electrical equipment, to get your guarantee you have to say what other electrical equipment you have had from this organisation. So all of that is happening, but they always do state in a little box at the bottom saying, “We can share this; do you object to sharing this information?” That, of course is a commercial issue, because they sell it. So I just wonder if we are getting too worried about the subjective nature of the way the data is collected and would it not be better to have everybody on the same database?

Mr Thomas: There is a lot of ground in the various points you have made. DVLA I think is a very good example where thought was given for putting in place an arrangement which is undoubtedly of huge benefit to the citizen – two minutes to go on line to renew your car tax rather than two hours queuing at the post office. But on that occasion the arrangements behind the scenes between DVLA, between the agency which looks after MOT certificates and between the private insurance companies are very important to make sure that that can happen and that the consent of the motorist is secured at the point they use the service. So it is done in a very structured way and I applaud that particular example. I think the debate about a compulsory DNA database for every citizen is a very big debate. Lord Justice Sedley came forward with something similar himself a couple of months ago. I did have some very strong reservations about that and I would be happy to elaborate on that if you would like me to. I think both for practical and civil liberties reasons I am really quite sceptical about the logic of saying that there are some unfair discriminations there at the moment and therefore we resolve that by having everyone’s database on a mandatory basis. I would just differ on that point. Your reference to Tesco and to the private sector brings out one of the fundamental points. Nobody forces you to shop at Tesco – you have a choice, you can go to Sainsbury’s you can go to Marks & Spencer or wherever and they all have a very strong interest in making sure that they treat your information properly. They safeguard your information as a very, very valuable commercial asset, so they have a self-interest in

safeguarding it but also a reputational issue, and in fact all the evidence that we have is that they take a lot of effort to make sure that it is kept safely. But in other areas of life, when you are dealing with social services, with the police, with the tax people, with immigration you do not have the same element of choice and I think that perhaps brings us into the arena of this Committee, the constitutional issues where, at the very least, there needs to be a great deal more transparency – picking up Lord Bledisloe’s point earlier about people needing to know where that information is held on them and what information is held. That is one of the very important principles of data protection, being entitled in most cases to see what is held about you. But it also brings us to the situation that if these developments are to take place there needs to be a great deal more public debate. So many of these have happened away from any real parliamentary or public debate or scrutiny; it is only in the last year or so that we have had these questions coming up on radio shows, on television programmes, and I think now people are beginning to wake up to some of the implications.

Q12 Baroness Quin: Just on a supplementary to that, where in your role do you have the responsibility to try and widen the debate? You did say that you were delighted to see an article in the *Mail* and in the *Guardian*. Do you have the sort of Information Commissioner’s PR as the judges do to do the right thing?

Mr Thomas: Yes, I have a statutory duty to promote good practice and there is no question but that part of that is raising public concern. I have a press office and we both proactively and reactively deal with the issues in the media as they come forward.

Q13 Viscount Bledisloe: Before I come to my question can I ask you one thing arising out of the point you made about my earlier point? Is it sufficient merely to say that you should have a right to ask whether you do have information about me on this because supposing I never was abused as a child, and I did not realise they thought I was in danger, should I not

actually be told in advance that there is this information about me rather than asking the question to which I think I know the answer?

Mr Thomas: David, I am sure, will say more about this. I will try and simplify the Data Protection Act in one sentence, which is that very generally you should either agree to or be told about the collection of information and then you are entitled to ask for the full details. So, as a broad proposition, where information is being collected you should know about it – not in all situations, there are some exceptions – but the right I mentioned is the right to see the detail, the actual file with the full details. David may want to say something.

Mr Smith: I was going to give an example where we did have a case which involved the Metropolitan Police, where again it was to do with applying to work with children and the first that someone found out that a complaint had been made about them was when it came out on the report when a check was made when they applied to work with children. We took the view that the Metropolitan Police should have told that person actively that the information was recorded. They came back and said, “But if every time we receive a complaint we have to go and tell everybody that is a huge amount of work,” and essentially the position we took was, “You do not have to tell anybody if it is just routine, kept in your records, a piece of your intelligence, but if you are actually going to use that and it is going to appear to be to the potential detriment to that person then you do have an obligation to actively tell them so that they know and they can challenge it if they think it is wrong.”

Chairman: That is very clear, thank you.

Q14 Viscount Bledisloe: Can I come back to my proper question? You quite understandably think that your influence on the formation of government policy before it gets to Parliament should be increased. How do you think that should be done? For example, do you think you should have a statutory consultative role? And do you think that you have power, if you do not have it already, to report to Parliament if you make an objection which is

ignored or overruled? And do you have the resources to cope with that if those powers were given to you?

Mr Thomas: We are very proud of our independence. It is a requirement of the European Directive that there should be an independent supervisory authority and I think it is very important that we are independent. But sometimes being independent has some drawbacks in that you can be out of the Whitehall loop and sometimes in the past – although I think things are changing – we have only come across things too late, as I mentioned earlier, and we have not been consulted to the extent that we perhaps think we ought to have been, and some departments themselves, I think, have recognised rather late in the day that they should have been in touch with us at an earlier stage. Things are moving forward; we have already touched on the possibilities of a statutory duty to consult outside generally or in particular situations. It could be done by some sort of amendment to the Data Protection Act giving a more general right to be consulted. It could be done on each Bill as it comes forward, on a case by case basis – I think there are options there. If the Committee would like we would be happy to write a paper and set out some more detailed suggestions. I do not think we are tied to a particular way forward.

Q15 Chairman: That would be very helpful.

Mr Thomas: We would be happy to do that. We do have the right to make a special report to Parliament – I forget the exact language, it is Section 52: “The Commissioner shall lay an annual report”, which we do every year “before Parliament. But the Commissioner may, from time to time, lay before Parliament such other reports with respect to his functions as he thinks fit.” We did that for the first time ever last year and I think perhaps with hindsight it should have been used more frequently. We produced a report called *What Price Privacy?* documenting the pernicious trade in illegal obtaining of personal information, and we may want to have another question on that later. That was an example of using, for the first time

ever, that power to lay a report before Parliament, and we did it with a follow-up report six months later documenting what had happened. You also touched on resources and you will not be surprised if I say that our resources are very limited and we cannot, I am afraid, churn out reports like that on too frequent a basis – we have to be quite selective in issues that we address. Equally, if we are to make reports to Parliament the more attention that such a report receives the more (obviously) we would welcome that.

Chairman: We have a lot of questions to ask you so we must crack on. Lord Morris has two questions.

Q16 Lord Morris of Aberavon: The Prime Minister’s recent speech in October discussed privacy protection and other values that might conflict with it, and he charged you and Mark Walport with the task of reviewing the framework for the use of the information and “to assess whether it is right for today’s landscape and strikes the right balance”. How do you view the terms and scope of this remit, and how do you propose to undertake this assessment?

Mr Thomas: Lord Morris, I have already mentioned my general welcome to the speech. There was a specific paragraph there which I learnt about the previous evening, that I was going to be asked to carry out this review of information sharing alongside Dr Mark Walport, who is the Chief Executive of the Wellcome Trust, and I very much welcome the invitation. This is to be a fairly quick review – we have been asked to report by the middle of next year – a report into information sharing, which I think will look at both the public and private sector. Mark Walport and I only had our first meeting last week. We will have a small, independent secretariat to support us. The two of us have decided that we will be issuing a consultation paper at the earliest opportunity, to identify the main issues and to seek a wide range of views as to the best ways forward. I think that the review will provide a fresh opportunity to look at some difficult information sharing issues and try to draw a line under a debate that has been going on now for some four or five years in a rather unfocused way and giving a clear

framework for the future. We have no preconceptions as to how the review will be undertaken but I think we are both agreed that information sharing as such is no panacea. Sometimes people think that just because you can share information you should do so and we are quite clear that that is not the right starting position; there should not be sharing of information just for its own sake. We equally recognise the values of information sharing for law enforcement, for improving public service transformation and so on. So what we will be doing is trying to identify where the boundary lines should be drawn as to what is acceptable and what is not acceptable and what safeguards should be put in place. Mark Walport was associated with a very welcome report published last year, which did not get very much attention. It was published by the Council for Science and Technology and that itself said, if I can summarise, that technology now allows so much information to be shared that we need to have much more awareness of this, and it said that just because you can share information you should not do so automatically. A very strong warning about the dangers of jeopardising public trust and confidence, and there was a very clear message there in the Council for Science Technology report that if you jeopardise public trust and confidence you may undermine the very purposes you are seeking to achieve. A very similar message came out in the Royal Academy of Engineering report. I think it is quite interesting that we have two sets of experts, if you like, the technologists, both saying that technology can do almost anything these days and the cost of processing has come down, the cost of storage has come down but just because you can do it, be careful.

Q17 Lord Morris of Aberavon: I suppose it is too early to ask how the consensus that you referred to might be reached?

Mr Thomas: I think it is, Lord Morris; we are just starting this review.

Q18 Lord Morris of Aberavon: The collecting of private sector data by government, what dangers do you see from that? Are they going to be different from the public sector?

Mr Thomas: I think we are all aware how much information the private sector collects on us now. Our research shows that people value the confidentiality of their financial information at a very high level and the bankers' duty of confidentiality has always been an important area. Credit reference agencies collect vast amounts of information; airlines and travel companies collect information; we have mentioned supermarkets; Google, the history of our searches; Facebook and other social networking developments. The amount of information about each of us now being shared and passed domestically and internationally is quite staggering, and it is not surprising that the police and the security services, other public agencies can see some benefit in some cases for having greater access to that. But we are very clear that there are substantial dangers in any sort of free for all. It is a fundamental principle of data protection that information collected for one purpose should not be used for another unless certain requirements are met. So we are not saying that there should never be access to private sector databases, but we are saying that it should be controlled. I have mentioned the Serious Crime Act, which is concerned with the fight against fraud and we think that the balance there is the right one. There has been a lot of controversy about the United States' Department of Justice accessing the international monetary transfer system, SWIFT, and that was done without any public knowledge and it came to light last year and with our European colleagues we challenged the way in which SWIFT was processing billions of dollars and pounds of transfers every day and that information was being made available within the United States to security services there. Changes have now been made; they have been announced publicly by SWIFT and by our colleagues in the data protection community to put a tighter framework around that sort of access to information. I do not think your question can be answered in black and white terms. If there are legitimate, well

defined purposes for accessing information, perhaps with proper authorisation from judges or in other ways to authorise it, that might be acceptable, but a free for all is not acceptable.

Q19 Lord Morris of Aberavon: What new powers do you seek?

Mr Thomas: Could I ask David to tell you a little bit about the proposals that we are putting forward to the Ministry of Justice about increasing our powers under the Data Protection Act?

Mr Smith: We have submitted a draft proposal to the Ministry of Justice. This is in two areas. One is to introduce a criminal offence for those who, broadly, knowingly and recklessly flout the data protection principles with a serious consequence. So say the doctor, the hospital that leaves the laptop in the back of the car with the patients' records on, it is hard to say that that is anything other than gross negligence. At the moment our power would only be to issue a notice to say that that should not happen again and if it happened again then there would be a criminal offence committed. That blatant breach of fundamental obligations should attract a criminal penalty. You can contrast it with the approach to security and the sort of information taken in the financial services sector, where the Financial Services Authority imposed the penalty and it was close on £1m on Nationwide, in similar circumstances – and I have to say not just because they had a laptop stolen but because that was illustrative of a lack of proper procedures. We are not seeking those sorts of powers but it is an anomaly that in financial services financial information, because of the risks to the market you can, as a business, face that sort of penalty, whereas if you fall outside those regulatory frameworks then all you fall back on is general data protection regulation where there is no penalty. The other area is a power to inspect. At the moment we can inspect the processing of personal data by organisations, public and private, but only with their consent – in only some very limited areas to do with European systems, Europol and so on, do we have a right to go in and say that we have come to make some checks. We are, as far as we can see, almost unique as a regulator in having a set of responsibilities to oversee and not then

having a power to inspect that they are being put into practice. We think it will concentrate minds. We would concentrate any inspection power where the greatest risk applies, and we would not be able to inspect thousands and thousands of organisations, but it would help, we believe, to deliver data protection compliance and to get business – public and private sector – to take data protection seriously.

Q20 Lord Lyell of Markyate: Very quickly, can we introduce a sense of proportion into this? I declare an interest, I have general practitioners in my family and they have to carry everybody's data about in their laptop. If they are going to be made criminals because they have made a mistake and leave it in the car you are out of proportion.

Mr Thomas: I do not think we would dispute that, Lord Lyell. The way we are putting forward the proposal is really quite narrowly focused and the example we have given is where a laptop with a lot of personal information is not sufficiently cared for and has not been encrypted. The technology now is available to encrypt a laptop and, frankly, any doctor and anyone else holding personal information should know the basics of making sure that the data is encrypted. Many examples of security breaches in recent years have brought home the imperative of that message. I am not seeking to criminalise a doctor for a single incident but when there has been gross negligence we need to have some sort of deterrent in place to make sure that people understand the importance of safeguarding the information. The proportionate approach is the one we are seeking to take.

Q21 Chairman: If I can move on to a different area, which you referred to implicitly a few minutes ago, which is the growth of these very unpleasant agencies who are parasitic upon the press in that they will obtain data nefariously or illegally which they then try to sell to newspapers as celebrity stories. I think I am right in saying that you reported in strong terms that people who indulge in this illegal collection of data should be subject to imprisonment

and not merely a financial penalty, and I think that forms clause 75 of the Criminal Justice Bill at present in front of the Commons, and I wonder if you would like to give us your thinking both on this practice and also what the appropriate response to it is.

Mr Thomas: Section 55 of the Data Protection Act, which in effect has been there since the mid-1990s, is the only criminal measure in the Act at the moment, and that makes it a criminal offence to obtain personal information from a data controller, someone controlling a database, for example, without consent. Over the years we have investigated a number of these cases and we have brought prosecutions for some serious matters, which have resulted in derisory fines. We published the parliamentary report I mentioned earlier in May last year to document what we have been doing in this area, the nature and the extent of this quite pernicious black-market – a whole network of private investigators with a range of clients, including some financial institutions, some law firms, some local authorities even and representatives of the press are also the ultimate customers for this black-market. We obtained so much information about these activities that we were able to publish a tariff of how much it costs. For example, to find out who your family and friends are with British Telecom was costing between £60 and £80; a vehicle check at DVLA £70; a company director search £40; ex-directory phone numbers £40; mobile phone account enquiries £750. So there was almost a tariff which we were able to put together from the information we seized using our search warrant powers. We prosecute and at the back of the report we document the results we get. I have to say that I was a very angry Commissioner when one of the most serious cases resulted in conditional discharges for all concerned. I thought it was wholly inappropriate that the courts, with only a limited maximum penalty, were not able to impose far more serious penalties. So we published the report and we, amongst other things, called for the penalty to be increased to one of imprisonment – six months in the Magistrates' Court and two years on indictment in the Crown Court. We said that we do not want to lock

people up but we do want a serious deterrent, and I am delighted that the government issued its own consultation paper following our report. Things have moved very fast indeed and as you said, quite rightly, Chairman, it is clause 75 of the Criminal Justice and Immigration Bill, which is currently before the Commons that does now contain provision to increase the penalties exactly in line with our proposal. It is not just that, we have also put forward proposals to the Law Society, the Financial Services Authority, the Office of Fair Trading, the Security Industry Authority, other bodies able to regulate this market far more tightly than has been the case so far.

Q22 Chairman: Have you included the Press Complaints Commission?

Mr Thomas: We have made recommendations to the Editors' Committee, which sits behind the Press Complaints Commission, but we have not been very enthused about their response so far. I spoke last week at the Society of Editors Conference and I had to say that, "I come here with my body armour on" because they had not been enthusiastic about this increase in penalties.

Q23 Chairman: These unpleasant vendors can only thrive if there is a market.

Mr Thomas: It is a supply and demand issue, Chairman. We have documented in our report some of the training manuals which we have found in some of these investigators' hands – they are the middle men, if you like. There are two main techniques they use. One is old fashioned payment – they find somebody inside the organisation, whether it is inside a phone company or police station or other areas where vast amounts of information are collected, and they make payments to people, or they blag. Blagging is the term used in this context, which is to either impersonate the individual or to impersonate somebody else inside the organisation. And as you amass more and more information about the date of birth, the mother's maiden name, the address, postcode, you can build up a picture and then, using that,

you can blag your way into an organisation. Another case is where they impersonate the organisation. The DWP in Humberside thought they were dealing with DWP in Belfast and for an hour and a half the person was on the telephone getting a lot of personal information before they worked out in Humberside that they were dealing with people who were not from the DWP inside Belfast. We have heard tape recordings of how they go about this business; it is a sophisticated business and we are very adamant that everything should be done to try and deter this sort of activity.

Q24 Chairman: Thank you very much. For those of us who have just only recently understood blogging, to get our minds around blagging as well is not easy!

Mr Thomas: It is “pretexting” in the United States; there have been a number of cases in the United States and in fact the Hewlett Packard Chief Executive had to resign because they were associated with this pretexting.

Q25 Lord Windlesham: You have really dealt with the question of the significance of the black-market. Do you think that the government should be doing more than it is and, if so, in what form?

Mr Thomas: Lord Windlesham, we are delighted that they have accepted our recommendation to increase the penalty, so full marks for doing that. I think also that the government is becoming increasingly aware of the risks. One of the first supporters of our proposal was the Department of Health. They are creating electronic health records. I think that something like 95,000 people within the health service will have access to those health records, and indeed the confidentiality and security around electronic health records is a major concern, and I very much welcome that. So they recognise that. First of all, they supported our call for increased penalties, but they also recognised the need for guidance and training and very clear messages to their staff about the risks of being duped by the blaggers and the

consequences which would face anybody who improperly disclosed information, whether for payment or otherwise.

Lord Windlesham: I might just say that I am very impressed by what you have been saying. I think for those of us who do not have any special knowledge it is an eye opener to realise both the significance of the problem and the action that is being taken. It is not an invitation for complacency but it is the comment that occurs to me without knowledge, having listened to this short discussion on it.

Q26 Baroness O'Cathain: Regarding the future development of technologies, do you think that technology designers and providers are sufficiently aware of the privacy implications, when you see these geeks, these 17-year olds being able to hack into computers all over the world, not fully aware of the privacy implications. But longer term, the people who are developing the technologies which derive from the experiments of these young people, how are you going to ensure that they are aware of the privacy implications?

Mr Bamford: Perhaps I can help you on that one? We do recognise that technological developments can provide the infrastructure of the surveillance society in many ways, and indeed the combination of different technologies in a technological synergy can bring about to actual increases in surveillance. An obviously example is CCTV and then you have automatic number plate recognition technology, which is then allied with a database to retain all the information of the vehicles and the vehicle number plates, and then you use sophisticated data mining software to mine the information out of that, at the end of the day you end up with quite detailed pictures of people's travelling habits and things like that.

Q27 Baroness O'Cathain: And trackers as well.

Mr Bamford: That sort of thing. So we see how technology brings together certain risks and threats. It does not have to be like that on its own. We are very keen in the data protection

community – and I think this is something which is gaining credence more widely – to deploy things which we call privacy enhancing technologies. The people who come up with all these technologies are clever people and they can think of more privacy friendly ways to actually process people’s personal information, and we have seen that, as the Commissioner referred to with the Council for Science and Technology report. Also, the Royal Academy of Engineers did a report on a surveillance society and they used a phrase there about how engineers should exploit engineering ingenuity to protect personal privacy. It is an idea that we could actually use technology in a way which provides some sorts of safeguards. To use an example in Europe, in Austria they have an e-government programme there which involves government departments sharing information between each other, but they do it on a basis of certain computer algorithms, which means that the government departments cannot see all the data that is held by the other department, they can only unlock what they need to in a particular transaction, and that is basically on the basis of an encryption key. That happens to be held by the Austrian Data Protection Commissioner in that country as a trusted third party to make sure it is used properly. There is an example of the big scale privacy enhancing approach. It can be done in a much smaller way – just putting encryption on a laptop is a way of providing some element of privacy protection there which is relatively simple and cost effective to do. We would hope that anybody who is developing technology and policy application should do it on the basis that they ask the people who are going to provide the technology to look at privacy friendly ways of using that technology. It is something which I think is striking a chime with the Department for Transport at the moment with its plans for road user charging, because they recognise that in theory you can build up a very, very detailed picture of vehicle movements as a result of a road user charging programme, and I do not need to explain to you the privacy risk that goes with that in terms of that big picture of how we all use our motor vehicles. They are looking at ways of doing this on a more privacy

friendly basis, to actually restrict the amount of information that might be generated and what might be available in other ways. To use examples of information blagging that have been referred to before, clearly if you restrict the information in a system which is on view to people who do not need to see it then the privacy risk of blagging is less because less people have access to it.

Chairman: Thank you very much. We are going to run out of time, sadly, with our distinguished witnesses, so can I ask both your Lordships and the witnesses to be relatively brief so that we can cover as much ground as possible? Lord Woolf.

Q28 Lord Woolf: I am afraid my question is a little bit technical but perhaps you can answer it shortly? Part of your role is to create best practice. Do you agree that there are, so far as the legislation within which you work at the present time, unclear definitions that could do with clarifying? And if you do take that view perhaps you could indicate whether in this respect the Data Protection Act might well be amended to do it?

Mr Thomas: I think the Data Protection Act has had a rather poor reputation over the years. It is seen sometimes as being rather technocratic, rather obscure in some of its language. I said earlier, Lord Woolf, that the fundamental principles are actually written in plain English and I think are robust and I think serve us very well to this day, and I think we should not lose sight of those. The approach my office takes is to take a practical, down to earth commonsense approach to the interpretation of the legislation, and our strategic aim is to help the vast majority of organisations who want to get it right and to be tougher on the very small minority who are refusing to get it right. We want to help people; we now issue a very regular programme of guidance notes, and we try to make sure that none exceeds three pages or so – very short, targeted on the small businesses, and we find the large businesses find that quite helpful as well, and also public bodies. There are debates which happen in the courts, amongst lawyers and amongst the academic community about, shall we say, the definition of

personal data. It is an important debate but perhaps only within those circles. It really only affects the very margins of our subject matter. On the changing definition – there has been a change because the European Commission felt that the UK interpretation as laid down by the Court of Appeal in the *Durant* case was not exactly the European Commission’s understanding, and we have attempted to square that circle now; there is an Opinion from the so-called Article 29 Working Party and my own office has offered fresh guidance, if you like reconciling the Court of Appeal approach with the European approach. But in real life this only affects matters at the margins. The definition of personal data in the vast majority of cases has never been in dispute. We also hang a lot of weight upon reasonable expectations. I have tried to share with the Committee today how we have to respond to the societal context. If there are clear, legitimate purposes for collecting information that is a very important input to the way in which we interpret the law.

Q29 Lord Lyell of Markyate: Can I just start by saying that I very much support your approach and your work and your personal approach to it and I am sorry I had to jump in and ask for proportionality, but it is important and you said so. You want the power to do what you call a privacy impact assessment. Could you explain that to us?

Mr Thomas: I will start and my colleagues will do a far better job than I can. Essentially we are going to be publishing a handbook in about three weeks’ time – we are holding a major conference in Manchester on surveillance society issues on December 11 and we have commissioned experts outside to help us develop a UK version of a privacy impact assessment. It is widely used in other parts of the world and it requires any major initiative, which is going to collect and use personal information, to go through a checklist as to showing how they have identified the risks, they have minimised the intrusion and they have put safeguards in place. So it is a checklist to ensure that some of the risks that we have been talking about this morning do not realise in practice. Jonathan is my expert on the subject.

Q30 Chairman: Could you make it the short version?

Mr Bamford: I will be a very brief expert on the subject, yes. Basically to deal with the original premise of your question, a privacy impact assessment would not be undertaken by the Commissioner's Office, it would be undertaken by the body who is developing the particular policy initiative because part of the process is deciding what to do so that they have a vision they need to get to and they use the privacy impact assessment ---

Q31 Lord Lyell of Markyate: I am just going to cut you short, if I may. Tell me somebody on whom you might impose this because it might frighten a small businessman who suddenly gets a privacy impact assessment.

Mr Bamford: The vision in our mind is not of a small businessman; the vision is based on other jurisdictions where it tends to be public authorities who are actually engaging in the use of information that applies to lots of people, used for potentially sensitive purposes like health. Obvious examples that we have touched on this morning in terms of public policy initiatives would be ones like ID cards, would be ones like in England, Connecting for Health and the wider use of patients' information beyond their own surgeries. We would have issues to do with road user charging. Those would be ones where you would use the privacy impact assessment. We do not think this is a tool for use with a small businessman. We think this is dealt with at public policy level in many ways. Of course, a major corporation such as a major supermarket with a loyalty scheme may want to think about a privacy impact assessment with something like that, and a credit reference agency might; but the corner shop, we do not think it is right for that.

Q32 Lord Lyell of Markyate: I think it is important to say that you are safeguarding the public and you do not want to become part of the problem.

Mr Thomas: Absolutely not.

Chairman: We have two more questions: Lord Smith and Baroness Quin.

Q33 Lord Smith of Clifton: Do you think that the general public understand what happens to their personal data when it is collected by government or by companies whether online or in more conventional ways, and what evidence do we have of public concern about privacy?

Mr Thomas: By happy coincidence, Lord Smith, we are publishing today the results of our annual track. Every year we ask exactly the same questions of the general public through a mass survey and the results show, undoubtedly, that awareness is increasing and concerns are increasing. People care about the subject matter; we ask people to rank their social concerns and this year “Protecting my personal information” has ranked second out of all the possible concerns. It is second to preventing crime; it is ahead of concerns about the environment; it is ahead of concerns about unemployed; ahead of concerns about education; and ahead of concerns about health. So it has gone right up the agenda. We know now that something like nine out of ten people, 90 per cent, have concerns about the security of their personal information. The figure about whether you have lost control of the way in which your personal information is collected and processed is that now 60 per cent are saying that they feel they have lost control over the way in which their personal information is being used. Again, if I may suggest, Chairman, we will send the full research results, which are being published this morning – we are happy to share those with the Committee.

Chairman: We are very grateful, particularly the longitudinal comparison for the way attitudes are changing would be very helpful. Baroness Quin.

Q34 Baroness Quin: My two questions relate to coordination. The first is between yourselves and other Commissioners, the Interception of Communications Commissioner, the Surveillance Commissioner and the Intelligence Services Commissioner and so on. Do you

have regular contact? Is there an overlap between the areas that you deal with and do you think that the coordination between you works?

Mr Thomas: Not very much contact on a regular basis because I think they have very discrete focused concerns which are not incompatible with our role – we co-exist perfectly well, we read their reports, we are aware of their activities and I am sure they read our reports – but we do not see a need for a regular programme of contact. But they have a very important role to play, the Surveillance Commissioner, the Interception of Communications Commissioner, the Intelligence Service Commissioner, but they are very specialised in their function – ours is a much, much broader remit. Your question also implied cooperation with our international colleagues because I think it is crucial to see these issues not just in domestic or UK terms. We all in the European Union work under the broad similar instruments at European level and we have very regular contact with our European colleagues, increasing contact now with our broad counterparts – it is not quite the same situation in the United States – but also Canada and Australia. A regular international Commissioners’ conference every year – we hosted it in London last year – took place in Canada two months ago. There is a huge debate about these issues in the United States, The Patriot Act, and phone tapping issues in the United States, surveillance by the FBI, security breaches, so what happens there is mirrored across here and vice versa – the debate is very lively over there as well as in this country. But I make no secret of my view that we need to have a far more global approach. I do not feel that we can have just a European approach; I think we have to find ways to reconcile the European approach with what is happening in the United States, in the Far East, South East Asia – all over the world, it is a global issue.

Q35 Baroness Quin: Are there any ways in which you have changed your own practice because of awareness of good practice elsewhere?

Mr Thomas: There are, yes, Baroness Quin. We published two months ago a data protection strategy setting out a more risk based approach to identify the detriments to individuals and to society, saying that we cannot do everything; we cannot adopt a conveyor belt approach, we are far more targeted now setting priorities, and we have developed that in conjunction with our colleagues elsewhere – they learn from us as we learn from them. The phrase we use is that we must all be “Selective to be effective”. I am sorry it is a sound bite but it goes down well around the data protection community – we cannot do everything.

Chairman: We are not opposed to sound bites. Could I thank you and your colleagues very much, Mr Thomas, and say how impressed I think we all are by the work that the Commission is doing and how grateful we all are for the full and very helpful evidence that you have given us, and I hope we can come back to you during the course of our inquiry when we need to. Thank you very much.