

WEDNESDAY 5 MARCH 2008

Present

Goodlad, L (Chairman)
Morris of Aberavon, L
Norton of Louth, L
O’Cathain, B
Rodgers of Quarry Bank, L
Rowlands, L
Smith of Clifton, L
Woolf, L

Witnesses: **Mr Peter Hustinx**, European Data Protection Supervisor (EDPS), examined.

Q466 Chairman: Mr Hustinx, good morning. Welcome to the Committee.

Mr Hustinx: Good morning.

Q467 Chairman: Thank you very much indeed for coming all the way from Brussels. You are most welcome here. We are not being televised but we are being recorded, so I wonder if you would very kindly identify yourself for the record. If you would like to make a brief opening statement before we proceed to questions, please do so.

Mr Hustinx: Thank you. I am Peter Hustinx, I am the European Data Protection Supervisor. Shall I briefly explain what my mission is?

Q468 Chairman: If you could please explain your role as the European Data Protection Supervisor and how it relates to the work of the Article 29 Working Party established by the 1995 Data Protection Directive.

Mr Hustinx: With pleasure. I have been appointed by the Council of Ministers and the European Parliament jointly as from January 2004 to be the first European Data Protection Supervisor, which is basically a data protection authority as they exist in all Member States but now on the European level, and that fills a gap, quite frankly, because national law did not

apply and before 2004 there was not an institution like this. I have three main roles, written out in more detail in the underlying regulation. The first is supervision, monitoring and ensuring compliance with data protection rules where they apply to the institutions and bodies, the Commission, agencies, the Council and Parliament, etc. That is about data processing by the institutions and bodies. The second role is consultation on legislation and policies with an impact on data protection. To be precise, whenever the Commission adopts a proposal for legislation with an impact on data protection it is under an obligation to send that proposal to me and my office for advice, which is then part of the discussion in Parliament and Council. I have developed the practice of being available for informal comments before that moment, and I give follow-up to the opinion in the discussions in Council and Parliament. So it is really consultation in the policy and legislative process as it proceeds. Thirdly, it is the role of co-operation, which is an under-statement because there is a soft co-ordination, long-term, promoting a consistency kind of co-operation - co-operation with national authorities and with the joint supervisory bodies in the Third Pillar. Much of this co-operation takes place in the context of the 29 Group you were referring to. I am a member of the 29 Group. Frankly, I used to be a member, before I was appointed EDPS, as the Dutch data protection commissioner.

Q469 Chairman: May I interrupt you there? Are you a member *ex officio*?

Mr Hustinx: I am a full member. If you read the text of the Directive it still referred, in 1995, to “an authority for the institutions”, but that is now beyond any doubt. So I am a full member. That co-ordination then takes place in the context of the group. In practice, the legislative opinions I issue are mostly some time before the 29 Group endorses it, sometimes it specifies some points which are relevant, say, from the national group (?); sometimes I am second, sometimes we decide to just bring this together in one document. That is a question

of timing, expediency or sometimes about the consensus. Overall, I am available and my staff is available on the ground on a daily level, and that is an advantage.

Q470 Chairman: How effective do you think the Article 29 Working Party has been in influencing policy and attitudes within the EU institutions and the Member States?

Mr Hustinx: Its impact on the policy-making is, I think, quite substantial. The 29 Group was designed as a mechanism in the Directive to provide for the so-called fine-tuning of the harmonisation approach. The Directive was a harmonisation instrument to make the intra-market (?) work better. It is not only a question of rules; it is also a question of practices. My activity since 2004 has certainly added, say, more substance, also, in terms of Third Pillar advice. That is a practice which has developed over the years. The Commission has welcomed it. I have offered it immediately, for the simple reason there is a lot of privacy in data protection issues around this, and it does not make sense to be very particular about drawing lines. So we do both. In practice, it is 50 per cent Third Pillar related issues and, also, quite a lot of issues about the interface between private and public. The same applies, I think, to my role. We have evaluated the impact of the legislative council and consultation. In the First Pillar it is very visible, particularly in the role the Parliament is playing; there is co-decision and the Parliament, really, uses my input to prepare the response. In the Third Pillar it is somewhat different, although I am not very disappointed, but there it takes unanimity under current rules, which will change, as you know, next year, probably. It takes unanimity to come to a conclusion, and that is in many cases a decisive condition for, say, less than optimal results, and data protection is part of that problem. So, for instance (and we might come to that), I have issued three opinions on the Third Pillar framework decision, and I must say I am not very pleased with the result which is likely to be the end of the discussion in the course of this year.

Q471 Chairman: Can I ask: what are the obstacles to greater influence? Why are you dissatisfied?

Mr Hustinx: Part of it is the institutional arrangement, but as part of the Lisbon Treaty that is about to change, provided that is ratified by all Member States. However, if that happens (and I think the signs are positive) then this means there will be co-decision of Council and Parliament. There will be qualified majority or simple majority voting, there will be arrangements for adequate transparency in what is happening, there will be some oversight by the courts, and all that provides for the usual arrangements which lead to better decision-making on substance and, also, on respect for fundamental rights. Now, you made the point that the present arrangements also lead to less than the best conclusions in terms of effectiveness. Co-operation is something which needs to happen intergovernmentally, with inter-police and inter-justice co-operation – it is just, I think, a great practical need. However, due to these arrangements we see that sometimes necessary decisions are difficult. On top of that, if negotiations take place between police services and police ministers then the language of fundamental rights protection is not always welcome. So you need checks and balances to make this happen, and I think you are very much aware of this. So I am quite hopeful that this will be better next year.

Q472 Lord Rowlands: You have just mentioned that the Lisbon Treaty dismantles the Third Pillar. The UK have opt-ins and opt-outs in that arrangement.

Mr Hustinx: I have noticed, yes.

Q473 Lord Rowlands: Therefore, I presume, that opt-in and opt-out will also apply to the whole of your field, and that, in fact, the UK will not come under the same surveillance that you look eagerly towards.

Mr Hustinx: Allow me to go step-by-step. First, yes, the Third Pillar structure will be lifted – dismantled. So, basically, there is a holistic approach. Some of the details of the Third Pillar interest, of course, are still then part of the decision-making. So it is not entirely changing, but the basic structure means that for the role of the Parliament (and there is no opt-out in that case), if it comes to the Charter on Fundamental Rights, there are some opt-outs, and some of them are clear in the Treaty, but, of course, what has been accepted is the *acquis* which provides for the general principles of constitutional issues of all the Member States. The case law of the court is not likely to change as a result. I am not going to speak about the opt-outs, but I think for the analysis I was giving, and comments I will make, I do not think it will have a great impact. So it is relevant for all the Member States. What I would argue is that it is a very helpful improvement of the constitutional framework; that difficult issues of balancing different interests and ensuring fundamental rights, in the context where they are most needed - to balance protection at least. That improvement is important and it will also help me in making the points I have made before, and I will see, I think, better feedback.

Q474 Lord Rowlands: Do you anticipate that the new remit you will be obtaining as a result of the dismantling of the Pillar will apply to the United Kingdom, as much as those who joined up to the *acquis*?

Mr Hustinx: My remit is on the European level, but as to the consultation on new legislation I think I will see more impact of data protection safeguards after 1 January, assuming that is the date, if only because the Lisbon Treaty itself clearly specifies the need for Article 16 of the second part, the Treaty on the functioning of the Union, which provides for horizontal safeguards, which now even are going to apply to the Second Pillar, but certainly to the Third and the First. That will lead to the need to revisit some of this and it will then happen with the full involvement of the European Parliament. That means, probably, most of all, the Committee on Civil Liberties - which is the Committee on civil liberties, justice and home

Affairs (that is an interesting combination) - are very much aware of the need to strike balances, because they do it all the time, and they are a keen supporter of adequate data protection safeguards. So my sense is we will see some improvement there.

Q475 Baroness O’Caithan: Mr Hustinx, you are reported as having said that “messages such as ‘no right to privacy until life and security are guaranteed’ are developing into a mantra suggesting that fundamental rights and freedoms are a luxury that security cannot afford”. Can you elaborate on this, please?

Mr Hustinx: Yes, with pleasure. This was a statement I made in June last year, in the last month of the German Presidency as an invitation to the Portuguese Presidency. I was addressing some concerns which had developed over that period in Council. Some particular initiatives which I thought had great impact on data protection, anti-terrorism measures, were not prepared in a very satisfactory way, but, also, there was a trend of representatives of important Member States, as well as members of the European Commission, alluding more and more to the fundamental right to security (which is an important interest which I will judge, but is not a fundamental right of itself) and saying that there is a right to life and liberty, but the discussion of a right to public security was seen to be more than just a coincidence. This happened in the context of various informal ministerial meetings, statements and speeches in the European Parliament, and I felt it necessary to just give a strong signal about the existing arrangement. There was also the statement, I think, of John Reid, at the time, that it was important to perhaps reconsider the existing framework - the constitution of the Convention on Human Rights needed to be reconsidered. I found that worrying and it was that context which made me say what you have just quoted. Could I be more precise? The present framework relating to privacy and data protection but to fundamental rights in general do not deal with these rights as holy stones not to be touched, not to be excepted from under any circumstances, but they proceed in terms of balancing on

the basis of very precise criteria. So the need for public security, for safety, is certainly a legitimate right, but you need then to specify what exactly is the purpose of a measure, and then the language. If it is necessary for that specific purpose and the law is clear - it is accessible, it is predictable and there are sufficient safeguards - then that measure is legitimate, but that then sets up, I would say, an agenda of tests which are to be met and demonstrated and verified, and this is how both courts in Luxembourg and Strasbourg (Strasbourg most of all, but both courts) proceed. This is what I apply in my advisory practice. The impact assessments which are usually part of these proposals are based on the same premise, but I am not always pleased by the way the impact assessment is done because the language is sometimes easy; we can say: “We think this is appropriate, this is effective and we think this is necessary; we think it is appropriate”. So that was the background against which I have made the statement. It then led to a meeting in September with the Portuguese Minister of Justice and I think he recognised, basically, what I have said and that they were keen supporters of the existing system. So this was part of the public diplomacy, but sometimes it is necessary to give that signal.

Q476 Baroness O’Caithan: I find your answer quite staggering, actually, I have to say, certainly, on the basis that everybody says now that security of the state and the protection of human people in the state come as number one. This is what people in a democracy actually believe – that our security is much more important than privacy. After all, the threat to security comes from the unknown and threats to our privacy are more known, and it is the fear of the unknown, of course, which causes the problem. I am really flabbergasted, I have to say, because I reckon if you went on national television and made that statement people would say: “It’s fine for them stuck in an office somewhere in Brussels to say they do not actually think security is that quantifiable and it is much better that privacy should come first”. That is the way it would come across.

Mr Hustinx: This is not what I said. I would not subscribe to that summary. It is not a question of importance under other concrete circumstances; the question is: where do you start weighing what is legitimate? There is no doubt that in 1950, when this was concluded, and it has been applied in a list of cases, this is the way the court has measured. In very difficult cases in the 1970s, dealing with terrorism in Germany, the approach of the court was: there is no human rights-free zone; even the most invasive measures to protect security have to meet certain tests. That was the background. What is the problem is that, in certain contexts, it seems that governments find it difficult to comply with all the consequences of the safeguards, but that is part of the legitimacy. I was concerned by the fact that the repeated use of the language was suggesting things like: “Well, a different order from the one we have”. If this was to apply to, say, a state which does not have any order, any security – a rogue state somewhere in the world – I would say: “Yes, let us first have some basic arrangements”, but this was not the thrust of the discussion; the discussion was, in Europe and the United States: “How do we proceed with measures which are designed to protect security and which are stated to contribute to security but we do not have the discussion to convince that this is really necessary under the circumstances?” It comes in waves, if we see no proper evaluation of the effects of previous measures. So, no, this is not just an office or a university lecture; this is about practice. In order to get to say privacy is part of the basic security all citizens have a right to enjoy, if we want to protect that society, we need to be specific. I am sure your Constitution Committee subscribes to that and it was against that background that I made my comment, and the comment was, of course, a public one, and that is sometimes very helpful to get points across.

Baroness O’Caithan: Thank you for that. The fact is, I reckon, we are probably all (well, I am anyway) thinking security equates with terrorism, and in fact that is probably the problem. To what extent do you think that the data protection arrangements within European

organisations or systems that operate in the field of cross-border policing and criminal justice are providing a high level of protection of the rights of citizens in the context of those functions? Do you feel comfortable with them?

Q477 Chairman: Can I make an appeal, please, because we have a lot of ground to cover and not much time, for fairly brief questions and fairly brief answers? Thank you very much.

Mr Hustinx: I will try but this is a very difficult question. There is in the Treaty a policy goal which is framed in terms of an area of freedom, security and justice (they are grand) being developed step-by-step, presently, and rules which are less than satisfactory. You have referred to them. What we often see is that this goes by steps, and I am concerned by the fact that some of these steps do not include sufficient – quite frequently it happens – parallel tracking, parallel progress, and there are some clear examples of this. In my view we should see co-operation of law enforcement between the Member States (that is crucial; I subscribe to that entirely) and see things like data protection safeguards as part of the necessary conditions for building trust in these very relationships. This is not only citizens; this is also, quite frankly, the police and law enforcement versus law enforcement. So, to make this more effective, more efficient, more adequate, you need to integrate data protection safeguards. That is a tool to make things better. Unfortunately, this does not happen in practice. Unfortunately, decisions are made on the assumption that sometimes they will be followed by adequate measures, and the Treaty, in Article 30, now makes this a condition. So co-operation, subject to appropriate safeguards. A clear example is the framework for the Third Pillar. The Commission proposed this three years ago but it has not been adopted yet. Its scope has been reduced, its content has been diminished and in the meantime arrangements like the Prüm Treaty decision are pushed forward. That is another interesting example because (you may come to this later in the Committee) the Prüm Treaty was designed as a testing lab for seven Member States which had, more or less, the same experience. Before the

first tests were really made, let alone evaluated, this was pushed up to a level of 27, and not with the parallel safeguards which you would expect, and I have made that point over the last year. This was part of the background of my comment on the mantra, and such like.

Q478 Lord Peston: You have referred to the Prüm Treaty.

Mr Hustinx: Prüm. It is a little place in Germany close to Luxembourg. It is like Schengen is, but that is Luxembourg. It is a little place where important treaties are concluded.

Q479 Lord Peston: Obviously, they are good concept places where important treaties are signed. You referred to it, and that takes us on to our favourite subject, DNA and mutual access to databases, and there are other provisions as well for the exchange of bio-information. Do you feel that this cross-border exchange of such information will one day have important effects on the lives of European citizens?

Mr Hustinx: No doubt, yes. No doubt. This applies to biometrics, DNA, fingerprints – all these things are extremely useful and interesting in police work. However, what is happening here is a huge infrastructure for setting up central databases in all Member States and providing direct access. That is not an easy thing; it involves 27 Member States providing direct access - it is an immensely complex task. What worries me is that we go from, in some cases, no experience at all with DNA to, in some cases, substantial experience with DNA. The United Kingdom is, perhaps, the world champion in DNA databases, but all this now in an environment where we have not thought sufficiently about how this should happen. So the Prüm Treaty was designed to be the testing ground and I am concerned that this is a less than satisfactory result. I predict (and I have stated repeatedly) that it will take a very long time before all this is implemented and we will see reports coming back in about this being delayed and we will hear the evaluation in the years to come. This is just a quantum leap in co-operation where we need to be doing this step-by-step and by learning from the experience.

This is an important message, I would say. We see it all the time: measures are being piled up and they are not being evaluated. Sometimes there is an overdrive: “This is important; we cannot wait; we need to do this now”, and the overdrive is the moment where risks are taken without sufficient evaluation because there is a perceived need to do something. Of course, we are not surprised to see a big deficit in implementation of decisions of the Council and, indeed, the anti-terrorism co-ordinator says: “A lot of my problems are that these decisions are not always implemented”, and that meets my point that we need to avoid overdrive, to do this step-by-step, with a keen focus on, of course, getting results, and data protection is part of that. The Prüm Treaty was an example of the scaling up of measures, and now, due to the fact that there is a lack of harmonisation as to the substantive rules - the rules in Germany, UK and France, let alone Bulgaria, Ireland, Denmark and Portugal, about DNA, who are not harmonised at all - if we start to access, to match, data on DNA, we will be confronted with all the complexity which arises from this diversity, and that is less than satisfactory. We will see in the courts arguments which could have been avoided in a more step-by-step approach. Let me make clear I am not against police co-operation; I am not against proper databases; I am not against direct access; I am not against biometrics being used, but it is just the overdrive and the problem of scale and the urgency which is the source of many problems – and, again, the lack of parallel tracks. If your staff check my advice in this context, I have made this point repeatedly.

Q480 Lord Rowlands: I think you may have partially, if not wholly, answered my question, and that is the cause of the delay in adopting the EU’s Framework Decision. Is it that, in fact, a greater priority has been given to security as opposed to privacy, and/or, as you have already indicated in answer to your first question, it is institutional because it was in the Third Pillar and not the First?

Mr Hustinx: Institutional is an important dimension but there is also, I think, in my view, a not fully justified concern that accepting common standards in this area seems to be very difficult. I find that puzzling because these standards already apply under a Treaty which all Member States have signed and ratified; it was the 1981 Council of Europe Convention on Data Protection. Furthermore, they have been translated in detail, specified in the First Pillar. Many Member States have implemented this Directive horizontally (that means including law enforcement) but coming to an agreement on the full scope framework decision is extremely difficult. So one way to come to a consensus is to accept a narrow scope. What does this mean? I am sorry to say that the UK was one of those who made it very difficult to have this large scope, and that is part of unanimity. The narrow scope meant that only when data moved to another country the standards apply, but they do not apply from the moment data are collected until the moment they are used, as will be appropriate for basic, common standards. The consequence is that for all practical purposes, for a number of years, all law enforcement authorities need to be aware of country of origin and country of destination, and if they have a complicated case involving three or more Member States they will have diversity and complexity in every case. So all their databases will now have to track and trace where data came from. You can imagine, that is not very efficient. Had they accepted a wider scope it would have been better, but it has not happened. It was extremely difficult to come to specifications of the right of access to law enforcement data. So my hope is that if we can now start from a less than satisfactory result and go back on the basis of experience, with the involvement of Parliament and co-decision, that is probably then the only way forward. It is worrying because this relates to important areas of law enforcement co-operation. It is about, also, the interface between the Third and the First Pillar, and your investigation, say, on surveillance society is internationally based on these two concepts. I find it very disappointing.

Q481 Lord Morris of Aberavon: I hope I am not reading too much into your answer to the third question about harmonisation to precede access, but from what I gather it has an effect on my question. Is there not a balance between security and individual freedom? You are critical of the use of passenger names etc. What is the basis of your criticism? Is it because of the element of the invasion of privacy or is it because of something deeper – the threat to civil liberties and constitutional rights? It could be both, of course.

Mr Hustinx: Yes, it is both, but let me answer at two levels. First, the concept of data protection was developed years ago to provide protection not only for the right to privacy but (this is a quote from the Data Protection Convention) “and other fundamental rights and liberties”, like non-discrimination, like free speech, monitoring how people read, how people express themselves, and fair process in a general way. There is a range of fundamental rights – the freedom to move is established. So it is not privacy in the strict sense; data protection is more inclusive. That is first. Second, applying the methodology I have applied for the last four years, which is based on the existing case law of the courts in Strasbourg and Luxembourg, I was struck by the deficiencies of the latest proposal on EUPNR. This was an example in which my opinion followed the 29 Group, and the 29 Group sums up 17 points on which it finds the proposal deficient, and I focus on four of them. The first, the major, is the legitimacy; the criteria of necessity and proportionality, and you look for the evidence in the proposal. There is hardly any evidence - it is very, very vague; it is anecdotal. The impact assessment does not provide any evidence on why there is a measure which is to lead to 27 central databases covering all airline passengers flying in and out of the European Union - all cases, no exceptions - a range of data. Why? Not to identify terrorists (because we have information on that), not to keep out people who are wanted; no, it is to collect information about everyone with a view to identifying possible risks and start to profile. That is a very, very far-reaching proposal which leads to the question of effectiveness. There is some

experience in the world that, in the case of the United States, was struck by the fact that the General Accounting Office of the Congress has raised lists of questions doubting the effectiveness of what is happening, and there is no evidence on all these levels. (See my opinion in detail for where this is supported.) So we say: “Shall we take a break to rethink this. Is this necessary? How are we going to deal with these data? Are they going to be exchanged?” That was the plan, and there will be a huge network of full surveillance of all airline traffic. Now, it is in that context that I made the comment (and it is at the end of the opinion) that this should be provided, in order not to end up in a total surveillance society environment. That was the context; the context was page 8, point 35 of that opinion – the conclusion. This is contrary to a rational legislative policy in which new instruments must not be adopted before those existing have been fully implemented and proven to be sufficient, and might otherwise lead to a move towards a total surveillance society. That is another big word, but that is the context. So, in my opinion, we should deal with important things in a serious and important manner, and this proposal, I think, is just not fully and seriously put. So it was probably submitted too early, and it could have benefited from that preparation.

Q482 Lord Morris of Aberavon: What you are saying is there should be a step-by-step approach?

Mr Hustinx: No, I am not arguing that we should move step-by-step to total surveillance, no, I am arguing that if a proposal like the one of EUPNR is made it should meet the test which applies to some huge operations, and that was a proposal of November. My opinion was given and within three months after that another package was proposed not only for all airline passengers but all passengers between now and 2015. So the waves of these proposals are profoundly worrying because they prevent proper analysis. I hope this analysis is going to take place and if this EUPNR proposal is not adopted before the end of December it will be

subject to the new rules, and we will do this in co-decision with full involvement of the Parliament. That will be a very beneficial step in this case.

Q483 Baroness O’Caithan: In view of the remarks you made in December 2007 about the ways to regulate the use of Radio Frequency Identification, do you see specific legislation as the way forward for every new technological development?

Mr Hustinx: No, most certainly not. I believe that the existing framework, Directive 95/46, is, say, largely still appropriate. I do not subscribe to the idea that this is outdated. What we should do now, first, is improve implementation. I find that it is necessary to think about changing that framework to make it more effective, and we need to prepare for this. That was my position in June/July last year. One of the things we should look at is the interaction with new technology. RFID is an example of this new technology. It is not a little gadget; it is identified as a major new trend which is to develop something which is now referred to as the internet of things (?). We will be likely to be seeing all objects like, say, telephones, razor blades and food, and so forth, being equipped with these little tags and they will be communicating, they will be tracing our behaviour on a daily basis. Against that background I say that we need to implement the existing safeguards to the full. Part of that is using privacy-enhancing technology, using self-regulation – there is a list of things we could do - but just in case this is not sufficiently effective we should now provide for some vital additions in the focus of RFID applications. I mentioned three examples of measures we can take in that opinion, but is rather a signal that I see the existing rules as effective provided we use them effectively, provided we do have proper awareness-raising activities, that we have provided for mechanisms to enforce this properly and provided we use privacy technology to the full, and so forth and so on.

Chairman: Mr Hustinx, thank you very much indeed for joining the Committee and coming all the way from Brussels to give evidence. I very much hope the rest of your stay in London will be enjoyable.

Memorandum submitted by Professor Bert-Jaap Koops

Examination of Witnesses

Witnesses: **Professor Bert-Jaap Koops**, Tilburg University Institute for Law, Technology and Society (TILT), the Netherlands, (via video link), and **Dr Lee Bygrave**, Associate Professor, Faculty of Law, University of Oslo, examined.

Q484 Chairman: My Lords, can I welcome to the Committee Professor Koops. Can you see us from your area in the Netherlands?

Professor Koops: Yes, I can see you. I can hear you, although the volume is not very high.

Q485 Chairman: We will speak up clearly. We can see you and you are very welcome to join the Committee. Thank you very much indeed for doing so. Also, welcome to Dr Bygrave, who is here in person, who has come to us from Norway. Could I ask, because we are being recorded, although not televised, if you could each give your name for the record and your position? If you would like to make a brief opening statement before we start questions, please do so.

Professor Koops: My name is Bert-Jaap Koops, I am a Professor of law and technology at Tilburg University. I do not particularly want to give an opening statement but I think I should say that I am a foreigner with not too much knowledge of the United Kingdom and so my evidence will be as an outsider looking at it from a distance.

Dr Bygrave: I am Dr Lee Bygrave; I am an Associate Professor at the Faculty of Law, University of Oslo. As you can probably hear, I am not Norwegian - originally I am from Down Under - but I have been based in Norway for the last 15 years, and am reasonably well-experienced with data protection law and practice in Europe.

Q486 Chairman: Thank you. Could I address the first question to Professor Koops, please, and do come in afterwards, Dr Bygrave, if you wish. Professor Koops, the United Kingdom is often said to have the most extensive surveillance of any liberal, democratic country. From your knowledge of other countries, do you think that assertion is valid? If you do not, could you give a more nuanced assessment of British surveillance?

Professor Koops: It is hard to say that the UK is a surveillance society more than other liberal, democratic societies at large because there are many aspects of surveillance. There are certain aspects, particularly, for example, the national DNA database, where the UK has probably gone further than any other country that I know of. However (and I am not sure it is a good example), on identity cards and identity numbers, I think, the debate you are having on identity cards shows that you are a bit wary of identity mechanisms as a surveillance measure, whereas many other countries have long ago introduced identity cards and identity numbers without any discussion. Another example could be wire-tapping, where, in Europe, Italy and the Netherlands have by far the highest incidence of wire-taps, probably – certainly in the Netherlands – much more than in the UK. It is difficult to give exact numbers. The entire system of surveillance measures is a sum of measures, and you have more of one thing and less of something else. We wire-tap more that means we infiltrate less. If I can give an overall picture, I think the UK is going far and fast; it is more extensive than most other liberal countries but there are certain aspects on which it certainly is not so much.

Q487 Chairman: Do you think these issues are taken seriously in the parliaments and national governments and institutions of the European Union?

Professor Koops: I am afraid I should say not always. Perhaps I should say more often it is not really taken seriously, from my knowledge, but there are exceptions. For example, in Germany, the Government and the Parliament is sensitive to privacy issues and to constitutional rights, but many other countries are a bit lax. Yes, they do pay attention to

privacy but they do not really feel privacy and other constitutional rights are really important, and they do not really do something with it.

Q488 Lord Rodgers of Quarry Bank: I have two questions, both to Professor Koops as well as Dr Bygrave. Are the effects of surveillance – we are talking about the United Kingdom – detrimental to civil liberties, human rights and the protection of privacy? I wonder whether you have any evidence or examples to illustrate your reply.

Dr Bygrave: I want firstly to just endorse what Professor Koops said in relation to the previous question and elaborate on one aspect there. If you look at the Scandinavian countries, you have had, for example, national personal identification systems in place from the 1950s and 1960s without very much discussion at all of the possible impact on civil liberties - indeed, the systems were just accepted as sensible, administrative measures – and yet that sort of initiative creates a lot more public debate here in the UK and, indeed, many other jurisdictions. So this, again, just shows that assessing the overall surveillance level of any one society, and comparing it to another, is a very difficult and treacherous exercise. At a street level, when I am wandering around London, I do not really notice any difference in surveillance from another European country, except, obviously, for bigger numbers of surveillance cameras. That is what is happening at street level, but I would say that equally if not more importantly is what is happening beyond street level, and there it is often very difficult to get accurate information as to what exactly is happening. It is also worth noting that in one of the most extensive comparative studies of surveillance levels and the regulatory regimes around surveillance, carried out in the 1980s by a Canadian professor, David Flaherty, the conclusion was that Sweden was the closest to being a surveillance society. That was a study published back in 1989. Professor Charles Raab is well acquainted with that study, so he could elaborate on it for you later. Flaherty's conclusion that Sweden was the most surveilled society was built, largely, around the very existence of this national personal

identification number and the extensive data-matching it facilitates. The UK, by the way, was included in that comparative assessment. Regarding detriment, obviously there is detriment to privacy if you regard detriment in terms of reduction of privacy. Surveillance, by its very definition, involves a reduction of privacy. The degree to which surveillance has a debilitating effect on one's perception of freedom and how one actually acts is more difficult to gauge. Bentham's Panopticon, as you all know, was premised on some knowledge of the control system in place, but that knowledge is often not present with surveillance measures, so people can, nevertheless, go around thinking they are free even though they are really in some sort of aquarium.

Q489 Lord Woolf: Do you think that the differences that exist between the UK and other continental countries are partly because of our lack of a written constitution, which would provide greater protection for the privacy of the individual and controlled data collection? I address that to both professors, and perhaps you, Dr Bygrave, would answer first.

Dr Bygrave: Well, it all depends on what is in the constitution, of course. Constitutional provisions for the protection of civil liberties can be formulated in many different ways, some of which provide, in effect, really just symbolic protection for the liberties concerned. It also depends on the type of judicial review that can be carried out on the basis of a constitutional protection. However, it is clear that if you look at, say, the Federal Republic of Germany, which arguably has the strongest protection for personal data in Europe, that constitutional platform has been very, very important for the case law of the Bundesverfassungsgericht in curbing, particularly, the latest spate of surveillance measures being issued by the interior ministry in the Federal Republic, and, also, at Länder level. I am not sure if you are familiar with the decision handed down just last Wednesday, 27 February.

Q490 Lord Woolf: No.

Dr Bygrave: It is a fascinating decision, not yet translated to English, but there the Federal Constitutional Court has struck down as unconstitutional a piece of legislation in North Rhine-Westphalia which was enabling covert online reconnoitring of internet activity. So activity like the covert placement of Trojan horses on someone's computer system would be, as a point of departure, unconstitutional.

Q491 Lord Woolf: Did it do that because it was disproportionate or on what basis?

Dr Bygrave: It was on the basis that it conflicted with the right to informational self-determination, which is derived from two very broad provisions in the opening paragraphs of the German basic law and which give the court a great deal of opportunity to review surveillance measures on a case-by-case basis. In this case they have been claimed to have invented a new right now, a right to protection of personal computer systems, though on the basis of this right to informational self-determination.

Q492 Chairman: Professor Koops, would you like to comment?

Professor Koops: Yes. I agree with Dr Bygrave that a written constitution is only useful if you have a good constitutional review. You should have a constitution with teeth, because just having a right on paper is not sufficient. I should also add that, obviously, we have a European Convention on Human Rights and Fundamental Freedoms which is valid for all European countries, members of the Council of Europe, and, through the Human Rights Act, is also implemented and valid in the UK, although I am not familiar with the particulars of it. The problem with, for example, Article 8, the right to privacy, in the European Convention is that there are exceptions to this right, which, although formulated very strictly on paper, (privacy can only be limited if it is necessary in a democratic society), in practice can be interpreted freely by governments saying, "We just think that it is necessary because we have much more organised crime", without any empirical evidence of what the need is. It is more

a matter of privacy being, as I said before, valued by practitioners, like High Court judges, and the source of privacy is not so much important. The example that Dr Bygrave gave is a good example of privacy being held up in Germany, not as much because it is in the constitution but because, for historical reasons, they really know the need, and other countries which have similar constitutions but do not hold privacy in such a high regard can much more easily interpret the words differently. So it is not really the lack of a political constitution in the UK that would be the most important factor of validity.

Q493 Lord Peston: I think my question is aimed mainly at Dr Bygrave but it may well be for our other witness as well. Until I sat on this committee and we did this inquiry, if you had said to me that you thought Germany was a freer society than our own, I would have said you are mad, and I think most people in this country would take that view; and if you were to suggest to me that the Swedes were a less free society than our own, with lots of Swedish friends, I again would have said you are mad. Is not the problem here possibly with the researchers looking into these matters rather than the reality, particularly the German case? I find it quite absurd that anybody would regard the existence of their constitution, or the example we were given, I think, last week that their railways could not issue a credit card because this might lead to the return of Heinrich Himmler. Again I would say, Germany had a terrible time and I understand why they have a got a constitution, but the notion that any of that is relevant to the problem of our society I find very puzzling, and I put it to you strongly that way so that you can respond, but what is your response?

Dr Bygrave: Certainly David Flaherty was accused by some people of being an outsider and not properly understanding the complexities of the jurisdictions he was looking at. Particularly Scandinavians reacted at his conclusion about Sweden and felt that he was being unjust, and that may be so. Nevertheless, I think it was a pretty honest attempt to make some sensible comparative considerations, and it was one that was done on the basis of extensive

interviewing and empirical research. He was not cutting corners, but obviously he stepped on toes with his conclusions. To get back to the point I made earlier, in every day life I do not think the quality of one's daily routines is significantly different in the UK to Germany to Sweden to Norway to Portugal. I think most people experience that they have a reasonable amount of freedom. A lot of the debates at research and policy level are about certain legislative initiatives that seem to fly over the heads of most people and, indeed, often never hit them, so that gives some of the debate a somewhat abstract quality, but, nevertheless, they are very important debates.

Q494 Lord Rowlands: I wonder if I could perhaps, Professor Koops, return to the constitutional point. In your very interesting appendix to the evidence you gave us in paragraph 8.3.2., where you discussed very helpfully data protection, you then say that there are data protection principles: "Constitutionalization of these principles ... is to be recommended." Can you elaborate on this aspect of constitutionalizing data protection principles?

Professor Koops: There are various ways in which you can approach data protection. We have a large body of data protection ground rules emanating from Convention 108 of the Council of Europe and with the European Directive outlining data protection principles. The fact that we said in our overview that data protection principles merit constitutionalization is that the instruments of data protection so far, the Data Protection Directive and the Data Protection Acts in most countries, are laws which can be interpreted broadly, and they are very complex and hard to implement laws and, because the instruments are so complex and hard to implement, hard to live up to, so it would help if you have a few, a handful of clear principles that say this is why data protection is important. Data protection is important because, in my view, it is about fair treatment, equal treatment, being treated fairly in social life, and that means that there are a few basic ground rules that you should live up to. The

data finalisation principle for example: you should have a purpose and you should stick to that purpose, and not use data for other purposes - one of the most important principles, I think - and should that be constitutionalised, although it is not necessary, it would be sufficient to engrain the need for such principles better in the minds of politicians and members of Parliament and governments.

Q495 Lord Rowlands: If you were doing that, how would you amend the UK Data Protection Act, by incorporating what, a series of principle statements? How would you do it?

Professor Koops: I do not think you can constitutionalize principles by amending the Data Protection Act, because the Data Protection Act is not part of the constitutional order.

Q496 Lord Rowlands: We have not got a constitution!

Professor Koops: I would not do that for this. I think in this case I would look, again, to the European Convention, Article 8. Data protection is part of that.

Q497 Lord Woolf: Do you not think that is a constitutionalized principle, Article 8 of the European Convention?

Professor Koops: Yes.

Q498 Lord Woolf: Does that not provide a constitutional base for judicial review in this country of data protection and data activities if the courts feel it is appropriate to do so?

Professor Koops: Yes, I think it does, but Article 8 of the European Convention is talking about data protection or is being interpreted as covering data protection in a very general way, it does not list the main principles, such as purpose specification and purpose limitation and audit and supervision. I think it could be sufficient, but it could help if the courts could also look at other instruments, like the Council of Europe Convention and like the European

Charter of Human Rights, which, through the new European Order, will become part of the constitutional orders as well of all EU countries.

Q499 Lord Rowlands: Professor Koops, how robust are current conceptions of privacy and the concept of a reasonable expectation of privacy in the face of what in your evidence you called a cumulative move towards surveillance? Again I read your appendix with great interest that in various constitutions the idea of privacy is written in Germany into the concept of human dignity, in France it is liberty, in Canada and the US it is search and seizure of property, et cetera. How robust is the idea of a reasonable expectation of privacy currently embedded in liberal society's legislation and constitutions?

Professor Koops: I think you should make a distinction between privacy, and privacy as it is known and used in the constitutions and in the debates in Europe, for example the ones you mention, and the notion of reasonable expectation of privacy, which is a more Anglo Saxon and American conception of privacy. Privacy traditionally is seen more as a fundamental right; whereas in the United States it is being interpreted as developing over time, and as people face less privacy on the streets, because they get used to cameras, they have no reasonable expectation of privacy any more, so there might be a consequence of the use of the notion of reasonable expectation of privacy that you gradually diminish privacy because technology in society tends to develop in ways in which people get used to less and less actual privacy. Instead of trying to read the notion of reasonable expectation of privacy into the constitution, as you mention, it might be more worthwhile to look at the, as you mention, notions of autonomy and human dignity as the underlying values of privacy and to use privacy in such a way. I am not quite sure whether this answers your question.

Q500 Lord Rowlands: Dr Bygrave, do you have any comment on that at all?

Dr Bygrave: While the notion of reasonable expectation of privacy is a notion that has probably been furthest developed by the US Supreme Court under its Fourth Amendment case law, we do find it, nevertheless, creeping into European jurisprudence. The Strasbourg Court is increasingly using this notion to assess what amounts to an interference with respect to private life under Article 8, paragraph one. In a case involving the UK, for example, the *Halford* case from 1995, the court was able to say a person working in their office is entitled to a reasonable expectation of the privacy of their telephone calls; so any bugging of the telephone which is without consent and, indeed, without knowledge is going to be interference. Whether that is a good development or not can be debated, and I would agree with Professor Koops when he says that the problem is that you introduce a slippery slide that is not particularly effective in the face of growing technology applications and people's customisation to these. So, if you can say, like Scott McNealy did, "You have zero privacy. Get over it", obviously there is not going to be much purchase for any right to privacy based on a reasonable expectation of privacy.

Q501 Lord Rowlands: If there is a kind of cumulative move towards surveillance, as Professor Koops stated, how will the regulatory agencies keep abreast with it and, as it were, defend the citizen?

Dr Bygrave: It is difficult. They are in a vulnerable position, because on the one hand they are under a statutory duty to uphold privacy and privacy-related interests; on the other hand they cannot adopt policies that are too far out of step with public perceptions of what is reasonable. We had this situation come to a head in Norway recently over a debate about whether video surveillance should be permitted on public transport where the Data Inspectorate, which is the equivalent of the Information Commissioner here, went out very strongly against such surveillance, and yet there were public opinion polls indicating that most people wanted the video surveillance, they thought it was reasonable, and they seemed

irritated over the more privacy-friendly approach taken by the inspectorate which was meant to be taken on their behalf. They did not want it; they wanted security.

Q502 Lord Peston: I am still worried a bit about the definition of privacy. Those of us who were brought up within the British education system and were taught essentially along the lines of what John Stuart Mill said thought there was an easily defined circle, at least Stuart Mill did, and that was the area of privacy, and his concept was that that was your business and no-one else's business. Am I not right that, largely for technological advanced reasons, you cannot draw that circle any more? Would you agree with that, that that is the problem, and that it has arisen, at least in part, from technology?

Dr Bygrave: Yes, partly technology, partly organisational or cultural practices in relation to technology. Technology never acts alone; there is always complex interaction between different factors. You see with the Strasbourg case law that you can have a right to respect for private life outside on a bridge going across a railway, so the public/private distinction is no longer as easily applied in the legal context as it was. Nevertheless, getting back to the Federal Constitutional Court in Germany, that has based a lot of its recent decision-making on this perhaps artificial notion that you do have an absolute private sphere into which the state cannot intrude, and that is particularly in relation to what happens in your own home, which is your castle, what you do in your own home with your friends, your family, in other relations of confidence, and that is a fairly definite border that the court has set up in an attempt to protect privacy interests against the ongoing development of technology and different organisational practices that would try to erase the public/private distinction.

Q503 Chairman: Professor Koops, would you like to add anything?

Professor Koops: Yes. I agree with what Dr Bygrave says. I should stress that I think it is no longer feasible to see this absolute sphere of privacy which is a close circle of privacy and

to view that in spatial terms, because even in your own home you can nowadays be monitored, and you are being monitored. For example, thermal imaging, the heat that the house radiates can be monitored from the outside and increasingly cameras can look through walls, and you have body scans that can see through clothes. So, even if you feel you are in your private space you can still be watched, with or without your knowledge, and I think it is important that we find ways to transform this notion of an absolute circle of privacy in which you mind your own business and the rest have nothing to do with it, to view that circle not in physical terms but in terms of probably data, who has access to what types of data and which data are really your own, and not only terms of data but perhaps in more flexible terms of space. It is a bit vague, as I said, but I think we should try and find new notions of what exactly is your home where you can be yourself. What is your castle in a world where the home is no longer restricted by four walls?

Q504 Lord Morris of Aberavon: We have referred to the European Convention, Article 8 in particular. I want to ask with regard to the role of the courts in clarifying rights. Is not the Convention a very important trigger mechanism in clarification? How is jurisprudence being developed, is it consistent, and is it possible to have an objective quantification? Which of the liberal democracies has the highest degree of surveillance and compliance with the Convention?

Dr Bygrave: I will preface my remarks by saying that, generally, the courts have not had a significant role in interpreting and applying at least ordinary data protection legislation. In Australia, for example, there was not one court case of any significance on the Privacy Act, which is the equivalent legislation to the Data Protection Act here in the UK, for 15 odd years; a similar situation pertains in Norway and in Denmark; a similar situation also has pertained in the UK, although we do now have an increasing number of cases, the *Durant* decision, for example, probably being the most significant in recent years, a decision of the

Court of Appeal, Civil Division. So courts have not had a significant role in clarifying the law in this area. Who has had that role? It has been primarily the data protection authorities through administrative decision-making, which has been somewhat problematic, I think, because in the first place a lot of that administrative decision-making has been poorly reported and, secondly, there has been perhaps a little bit of bias in the way in which those authorities interpret their respective pieces of legislation, which is inevitable, because they are there to uphold privacy interests, so they are going to interpret their legislation in a privacy-friendly way, but when the courts have come in, they have come in often as a corrective, and a welcome corrective, I must say. They have stirred up the cosy club of data protection authorities and said, “Hey, no, you cannot necessarily interpret this particular provision in this way. In fact this is the better interpretation.” One problem, though, is that the courts have not always developed a consistent line themselves. Look at the notion of personal data, which is a key notion for application of the Data Protection Act here and equivalent legislation elsewhere in Europe. We have, on the one hand, the *Durant* decision from the Court of Appeal, saying that personal data, as a concept, should be read down to only embrace data that implicates, as it were, the privacy of the person to whom it relates. On the other hand, we have courts elsewhere saying, at least indirectly, “No, that is not the case.” There are some interesting decisions over the status of IP address data. For instance the Paris Court of Appeal has held, “No, IP address data is not personal data”, whereas the Stockholm Administrative Court has held, “Yes, it is”, with the Data Protection Commissioners in the form of the Article 29 Working Party agreeing with the latter. So there is great uncertainty over how to interpret a key notion in data protection law. Fortunately, we have Strasbourg, which is increasingly laying down a set of basic principles that apply to the data protection field, and those principles are now being applied by the European Court of Justice when interpreting the Data Protection Directive. The *Rechnungshof* decision is the leading case there, a decision of the

European Court of Justice from 2003, saying you cannot interpret the Data Protection Directive without looking at the Article 8 European Convention on Human Rights case law. So Strasbourg increasingly is the baseline, at least here in Europe, but Strasbourg case law in itself is not always consistent and there are gaps and in some cases the case law has not come as far as the data protection legislation existing at national level. The right of access, for example, pursuant to Article 8 of the European Convention on Human Rights is much more restricted than it is ordinarily under data protection law at national level. That is quite a long answer. Maybe Professor Koops wants to supplement that.

Q505 Chairman: Professor Koops, do you want to add anything?

Professor Koops: Dr Bygrave has talked largely about data protection. We should stress, of course, that Article 8 also covers privacy of home and family life and correspondence and there, like with data protection, the European Court of Human Rights increasingly has many directional verdicts which are used by all the national courts, but, again, there are gaps there. How important is the jurisprudence for the overall protection of privacy? It is important, obviously, because it adds directional value, it guides the way that you should interpret privacy rights, but I fear surveillance is moving towards a paradigm of preventative measures in which you monitor large groups. This has effects on privacy, which diminishes the privacy of ordinary citizens, but that type of monitoring and surveillance rarely gets to the courts because it is preventative, and it might only get to the courts when people complain or when an odd thing happens, but the overall diminishment of privacy is just something that happens that is not brought in any case.

Q506 Lord Peston: Obviously you have been dealing with this in this way because Lord Woolf asked you a question about the courts, but speaking as a democrat, albeit a member of a totally non-democratic House, surely the real place for debating, guaranteeing is too strong,

but at least clarifying concepts like privacy must be the parliaments rather than the courts. I am rather troubled. Courts have to interpret what parliaments have put forward, but in the end parliaments are what matter, it seems to me. Do you agree with that?

Dr Bygrave: Yes, I certainly agree with that. The general problem with the courts is, obviously, the democratic deficit which in theory you do not have with parliaments. The problem, nevertheless, is that parliaments in the present climate, with a war on terror going on that seems to have no end, are not necessarily acting as a sufficient corrective to the push for more and more security, and that corrective is coming both from the Data Protection Commissioners and from the courts. I would love to see the parliaments being a corrective in this area, but at least in some jurisdictions they are not. Rather you have political parties outbidding each other to be strong on the war on terror.

Q507 Chairman: Professor Koops, would you like add to that?

Professor Koops: Yes, I think that we need the courts to steer, to control, to supervise what the parliamentary legislature is doing, because there is such a wide scope of interpretation for the privacy rights. As Dr Bygrave was saying, in the current climate it is easy to say, well, in this case the privacy, although important, should weigh less than a security measure. I think there are two particular points of contention for parliaments which make it difficult to really hold up privacy. One is that – and this may be different in the UK but at least in the Netherlands and I think in quite a few other parliaments they are incident driven. They are talking about what is important now and so they are talking about a single measure which seems important because with this you can prevent what happened last week, and so they look at each single measure, at each individual measure and, thus, do not have the overall picture and disregard the cumulative effect which all these measures together have on privacy. The second point of contention is that we are often talking about complex measures, computer technologies, and the precise functioning and what the technologies can do requires some

knowledge of technology, which again in the UK, members of Parliament may be an exception, but many do not know much about what technology does, so they have people imagining what the precise effects will be of implementing these technological methods, which is particularly important when building infrastructures with large-scale technology that is put in in society, such as surveillance cameras, biometric passports, which once there are hard to reverse.

Q508 Lord Smith of Clifton: It is very interesting. You have talked about the courts and the regulatory agencies and the parliaments but you made no mention of those vital parts of civil society which are the informal pressure groups, and they make up the democratic deficit to a great extent as guardians of civil liberty. Have there been any studies of the role of pressure groups across the EU Member States with particular interest in protecting civil liberties?

Dr Bygrave: I am not aware of any systematic study. I would suggest Professor Raab may be better placed to answer that question than myself, but you have made a very important point. Those sorts of pressure groups tend to be most prominent and vocal in the USA, where we have, for example, the Electronic Privacy Information Centre and the American Civil Liberties Union. These are actors that have an important role to play, although the degree to which their efforts ever result in concrete legislative action or concrete legal policy is debatable, but they are important in igniting public debate. I notice in Scandinavia those sorts of organisations do not have the same sort of role. People trust government to do that sort of thinking for them - misplaced trust in my opinion.

Q509 Lord Smith of Clifton: Hear hear!

Dr Bygrave: Here in the UK one has Privacy International, but that is effectively a three or four person operation.

Q510 Lord Smith of Clifton: There is No2ID and there is Liberty, of course.

Dr Bygrave: Yes, Liberty has played an important role in many policy areas.

Q511 Chairman: Professor Koops, would you like to add anything?

Professor Koops: I agree that pressure groups are very important because they can play a role in debates by giving information, by highlighting possible effects that in the general debates tend to be overlooked, but, as Dr Bygrave mentioned, internationally they are usually quite small, with a few people, often volunteers, with limited resources, and so there are only a limited amount of topics that they can monitor. More importantly, if the question is: do they not fill up the democratic deficit to a large extent? No, they never can, because they have no power. Their function is to highlight evidence, to signal, to give information, but they have no influence directly, they very indirectly have influence, but they have no power to say this measure should be not adopted, like parliaments, like the courts and data protection commissioners have, so they could never fill up the democratic deficit.

Q512 Baroness O’Cathain: How important is it to have a well resourced and independent regulatory authority for enforcing data protection, privacy and for keeping surveillance under control, and is it actually feasible to have one regulatory authority making sure that all three are treated equally?

Dr Bygrave: I think it is important to have a well resourced and independent regulatory authority. There is no question: such authorities do make a difference. I can point to many concrete examples where authorities, such as the Information Commissioner and his staff, or her staff, as it used to be, have come in and made a difference to concrete policy being rolled out. In Norway there are numerous instances where the Data Protection Authority has put a stop to fairly controversial plans for data-matching, not just within the public sector but also the private sector, and they have been able to do so under a scheme which, basically, meant

that lots of these controversial projects had to be approved by the authority in the first place. That sort of scheme is not always easy to put in practice because it is very bureaucratic and it is demanding of resources and these authorities are not usually well resourced. That is the big problem: they are not well resourced. Getting back to our friend David Flaherty, who I mentioned earlier, he came with a comment in his study which questioned whether such authorities were always a good idea. He said such authorities may, in fact, add legitimacy to surveillance measures, if they function effectively as a rubber stamp approval process where they can say, “We approve this process”, but they have not had the resources or the guts to go in and make a very good and sound assessment. But that is also a criticism you could mount against data protection law and other pieces of law that are ostensibly upholding privacy interests and giving citizens the feeling that, yes, privacy is being cared about but really do not have much bite. As I said, there are nonetheless numerous instances where data protection authorities have made a difference. An interesting point also, I would say, is that you just do not need a well resourced and independent regulatory authority, but you also need one with effective powers of intervention. Those effective powers of intervention do not necessarily have to flow from a scheme where you get prior authorisation from such an authority before you can proceed with data-matching or data surveillance practice. Flaherty’s study showed that, indeed, the German data protection authorities, which really are only ombudsmen, in the Scandinavian sense at least - they can only make recommendations - nevertheless, because of the particular personalities of these officers, their persuasive powers, their networks, were able to stop or at least dampen some of the surveillance efforts. Two other points. One is that you cannot rely solely on the courts. Court litigation to uphold your rights is, for most people, just too expensive and it is too time-consuming, so you need another avenue, you need another friend, as it were, to bring your complaints to, and data protection authorities are very well placed to be that type of body. You need also a voice in

international fora to thrash out privacy policy; and more importantly you need a body that plays an educational role. In other words, I would say you do not just need a well resourced, independent regulatory authority with effective powers of intervention, but you also need an actor that has an educational role and undertakes that role seriously. A problem so far is that these authorities usually have not had the resources to undertake significant educational efforts. There have been some good initiatives. The 'Protecting the Plumstones' CD-ROM that the Information Commissioner was responsible for producing and sending to schools here in the UK is a very good example of educating young people about civil liberties, about privacy problems with respect to ICT, et cetera, but we need more of those. Finally, legally it is a requirement to have at least an independent regulatory authority. The Data Protection Directive specifies this in Article 28. And if you look at the provisions encapsulating the new right of data protection that Professor Koops referred to earlier, you will see that the third paragraph of those provisions states, in effect, "Compliance with data protection rules shall be subject to control by an independent authority." This is in Article 8 of the Charter of Fundamental Rights from 2000 and in Article II-68 of the European Constitution from 2004, which will probably never enter into force.

Q513 Chairman: Professor Koops, would you like to add anything?

Professor Koops: I would like to stress the point that Dr Bygrave made that regulatory authorities should not only be well resourced and independent, those are two fundamental points, but should particularly have strong teeth and sanctioning powers. I would add that I see two functions for regulatory authorities: one is to supervise the way that data protection law and also privacy law is being implemented and lived up to in practice - that is one type of activity - but I think the other role could be equally important, and should be equally important, which is to provide parliaments with advice on intended legislation, which is the role that at least the Dutch Data Protection Authority has and, I presume, many other data

protection authorities as well. The problem is that they have no sanctioning powers about their advice and often what you see is that the Government says, “Yes, we have read the advice. It is all very nice, but we think differently, and so we just go on with this surveillance measure”. If Parliament does not then stand up and say, “We take the advice of the data protection authorities seriously”, there is no real effect on privacy and protection data, and so in some way advice from such a regulatory authority, if it is within the legislative process, should have a real value and weight, otherwise it is not much use.

Q514 Baroness O’Cathain: You say that the regulatory authorities should supervise the information being implemented and advise Parliament and do a bit of pre-legislative scrutiny, but surely is there a third role which would be to be independent and start an investigation of their own if they feel there is something going wrong?

Professor Koops: Yes, but I think that is part of the first role in supervising the implementation. They can do that in two ways: one by a complaints process, and so it is a reactive role, but there is a proactive role, “This branch might be a bit fishy, let us look into it.” We should also have an authority that looks at: does not the state do things which warrant looking into echelon-type of researches? I think that would be a good role, but it is not necessarily the regulatory authority, data protection authority that should do that.

Q515 Baroness O’Cathain: I really had one idea, and that was if something was being done, say, in the states or in one of the countries in Europe which had not actually spread over to the other 26 European Union countries, the regulatory authority in country A could say to the Government, “Really we ought to look at this. We want to look at this”, and then recommend. That is a proactive, which I think is not quite covered in what you said about supervising information being implemented.

Professor Koops: That would be a very useful function. It is not necessary to have the supervisory authority in that role. It might also be members of Parliament who trigger such things. For example, in European parliaments you often see that it happens in that way.

Q516 Chairman: Professor Koops, can I thank you on behalf of the Committee for your virtual presence with us and the evidence which you have given, and Dr Bygrave for coming all the way from Norway to be with us and for your evidence. I hope that the rest of your stay in London is enjoyable. Thank you very much indeed.

Dr Bygrave: Thank you, my Lord Chairman.