

WEDNESDAY 28 NOVEMBER 2007

---

Present

Bledisloe, V  
Goodlad, L (Chairman)  
Lyell of Markyate, L  
Morris of Aberavon, L  
O’Cathain, B  
Peston, L  
Quin, B  
Rodgers of Quarry Bank, L  
Rowlands, L  
Smith of Clifton, L  
Woolf, L

---

**Memorandum submitted by Surveillance Studies Network**

**Examination of Witnesses**

Witnesses: **Professor Clive Norris**, Professor of Sociology, University of Sheffield, and **Dr David Murakami Wood**, Lecturer, School of Architecture Planning and Landscape, Newcastle University, examined.

**Q36 Chairman:** Professor Norris and Dr Murakami Wood, may I welcome you to the Committee and, in the case of Dr Murakami Wood, may I welcome you back to the Committee as I think that you participated in our seminar. May I ask you formally to identify yourselves for the oral record, please.

**Dr Murakami Wood:** My name is Dr David Murakami Wood; I a lecturer in town planning at the School of Architecture Planning and Landscape at the University of Newcastle upon Tyne and a researcher at the Global Urban Research Unit.

**Professor Norris:** I am Professor Clive Norris from the University of Sheffield. I am Head of Department of Sociological Studies and Deputy Director of the Centre for Criminological Research.

**Q37 Chairman:** Thank you very much indeed. You are very welcome and we are most grateful to you for coming. I said to the Committee that we have a large area to cover and I have asked that questions be brief and so, out of fairness, perhaps I could ask that replies should be fairly concise too. Gentlemen, your expertise is in the field of surveillance. Are you able to say how easy it is to define “surveillance” and to what extent it is possible, if at all, to break the concept into subcategories?

**Dr Murakami Wood:** There are a large number of definitions of surveillance, some of which would seem to cast almost all information gathering as surveillance and some of which would seem to only argue that “bad” forms of information gathering are surveillance. I think we would regard neither of these extremes as being useful definitions. We would argue that the intentionality is the important aspect. I think that information gathering with the intent to influence and control aspects of behaviour or activities of individuals or groups would be our working definition. So, it is the intention that we regard as important. However, we also argue that not all data that is gathered with no surveillance intention cannot become useful for surveillance in future and also there is the question of unintentional consequences of information gathering that are not thought of when the information is gathered.

**Q38 Chairman:** We are considering both surveillance and the use of personal data. To what extent can public sector use of databases of personal information be seen as a form of surveillance?

**Dr Murakami Wood:** In a brief sentence, we would say that it is possible to conceive of a database that is not used for some form of control. That is perfectly clear. However, it is equally impossible to conceive of one that could not be and I think that statement is about as far as we can really go with that.

**Q39 Chairman:** Are you able to say in what ways and to what extent surveillance by the state can contribute to public safety in general and be helpful to the individual?

**Professor Norris:** The state is responsible for providing security and clearly there is a whole range of people who may be considered a threat to that. So, databases of known individuals who are active in terrorism, drug dealing and so forth seem highly appropriate and I do not think anyone would want to argue that they are not. So, in the sense that the state has a duty to protect and to gather information of those it has good reason to consider to be a threat, then I think that one would say that this of course can lead to enhanced security and safety. I think it would be silly to think that surveillance is a “bad” thing or that the construction of databases in themselves is a “bad” thing. They have their uses and their places. For instance, the Sex Offenders’ Register may be considered one of those things in general although, in its particular operation, one might have criticism of it. In that sense, there is not an argument that databases in themselves are problematic and they clearly can help in the administration of public safety.

**Q40 Chairman:** Are you able to tell us what information there is that CCTV has been as effective in deterring and detecting as was originally envisaged?

**Professor Norris:** “Little” I think is the short answer. When CCTV was first introduced in this country, it was not subject to systematic evaluation. It was introduced on the basis that practitioners thought that it was effective. Over the last ten years, studies have been carried out by academics and particularly the work by Jason Ditton in Glasgow and the work of Professor Martin Gill at the University of Leicester, which suggests overall that it has a very, very weak influence on reducing crime. The Gill study was published in 2004; it was the first major Home Office sponsored evaluation. Not only did it show that CCTV had very limited impact in reducing crime but it had very limited impact in reducing fear of crime. The evidence in terms of general reductions in crime and general reductions in fear of crime

appears to be very, very weak. There are studies that do show a reduction in specific places. For instance, the same team that looked at Glasgow, the Ditton team, looked at Airdrie and, in Airdrie, they did find a reduction. In Glasgow, they found that crime increased when CCTV was introduced. One further study that is worth mentioning is the Farrington and Walsh meta-evaluation which also found very weak evidence for CCTV as a crime reduction measure; this again was sponsored by the Home Office. If I remember correctly, they suggested at best about a three per cent reduction mainly in car parks and very little evidence that in town centre space you would see a reduction, but that street lighting seemed to be a rather more effective form of prevention.

**Q41 Baroness O'Cathain:** I have a very simple question particularly relating to your point about the fear of crime and showing that reductions in crime have not been affected by CCTV. Do you have any statistics at all about the reliability of these CCTV cameras? What proportion do you actually think are working? How many of them break down? Where do the manufacturers get a licence to produce them? Is there a special code or a specification for putting these up in the first place saying that they have to reach certain standards or can anybody string together some sort of camera and pretend that it is a CCTV camera?

**Professor Norris:** The answer to the first part of the question as to how reliable they are and whether there are statistics to tell us that, I do not know of any broad-range statistics on how reliable they are. Clearly, if you look at the Gill study of the implementation of range of systems, there were problems with reliability of systems and they were part of it, although I do not think they were necessarily wholly undermining of the systems but there were technological problems. The second part ...?

**Q42 Baroness O'Cathain:** Is there any organisation which actually looks at the manufacture of them, the actual physical specification?

**Professor Norris:** Certainly the Home Office has tried to issue guidelines.

**Q43 Baroness O'Cathain:** Tried to?

**Professor Norris:** Yes. I cannot answer your question with any certainty other than to say that they do issue guidelines as to what would be necessary in the technical sense. I think that the problem is that the range of possibilities is actually rather great, so specifying very exactly in any particular case what you can put in place and where is not such an easy job. One of the problems that has beset in a sense partly the expansion of systems is the problem of inter-operationability: different systems even in the same town and even run by the same council have different technical requirements, they do not integrate properly, and this still besets the industry.

**Q44 Chairman:** Do we understand from your answer to the first point of Lady O'Cathain's question that the reports we get in the newspapers of the number of cameras and the number of times we are all photographed are guesses and not based on any statistical evidence?

**Professor Norris:** I have to put my hands up to this because I am the originator of both these numbers. The number of 300 times a day that we are captured on film was included in a book I wrote called *The Maximum Surveillance Society*. Is it a guess, just a guess? I would say that it is a guesstimate. How I came to that figure was that I took a person in London moving around the City from early in the morning until late in the evening and I constructed a journey that intersected with known CCTV systems. So, this was not a fantasy in that sense, this was a journey. I think that I wrote this in 1998, so nine years ago, and I think that the estimate of 300 cameras was perfectly justifiable on what I knew about each of the systems that they intersected with.

**Q45 Lord Rowlands:** I am a little surprised by your initial answer because, for example, I travelled in on the number 24 bus this morning and inside the bus was a noticing saying that there was a CCTV camera and that there had been 60 prosecutions for vandalism. If you had polled that bus this morning, I would have thought that the vast majority of us would have said that it was an acceptable form of surveillance.

**Professor Norris:** I was not saying that it was acceptable or unacceptable, it was a question of how many there are.

**Q46 Lord Rowlands:** Yes, but you also implied that it was of very little value.

**Professor Norris:** I am saying that the best scientific evidence that we have does not suggest that CCTV surveillance is very effective at reducing general levels of crime.

**Q47 Lord Smith of Clifton:** Was this journey a journey which a number of people make or was it in search of CCTV cameras? Was it a deep search as opposed to a journey from Richmond to the City which a stockbroker might make?

**Professor Norris:** It was a busy day in London and it was trying to make a point so, in that sense, it was a piece of rhetoric. However, let us take my journey yesterday from the University of Sheffield to my hotel in London. Every stage of that journey was captured on a CCTV system. My university system captured me; on the bus that I caught to go into Sheffield to get to the station; as soon as I arrived at the station; I was captured when I got off at St Pancras; I was captured when I walked through to King's Cross, I was on their system; I walked into Smith's and I was on their system; I got into a taxi in London and that had a CCTV camera; I got dropped off at my hotel and, as soon as I walked into the entrance of my hotel, I was captured on a CCTV camera.

**Q48 Lord Smith of Clifton:** That was roughly 20 times; it was not 300.

**Professor Norris:** How many cameras are there? If we talking about the number of cameras that could have seen me, in the Underground there are thousands of cameras; in the stations there are thousands.

**Lord Peston:** I would like to ask a technical question following on from Lord Rowlands. Surely on Lord Rowlands' number 24 bus coming down from Hampstead no doubt.

**Lord Rowlands:** Coming from Pimlico.

**Q49 Lord Peston:** No one at the time you are travelling is a vandal, so that really does not count as evidence. The real point is that the vandals will be getting on later and they are not affected by those cameras. They are drunk, hooligans or what-have-you. Therefore, it is quite compatible that none of you were misbehaving but that the cameras had no impact on those who had a high propensity to misbehave. We do not know that, but we have to do the research and what we are being told is that the research shows that those who have a propensity to vandalise buses are not affected by the cameras. That does not surprise me at all.

**Dr Murakami Wood:** It is important to stress that neither Professor Norris and myself would argue that cameras are ineffective at adding to the weight of evidence or being used in court. I do not think we are saying that. The question was about prevention and the claims that were made for cameras when they were first introduced to actually reduce or prevent crime and I think it is quite clear from the evidence that we have seen that there is not enough evidence to suggest that there is any statistically significant effect on the rates of crime or any kind of crime prevention and that is the important distinction. It is up to you to make the judgment on whether that is important or not.

**Q50 Baroness Quin:** What evidence is there for displacement? In other words, if you have cameras in one place, crime just moves elsewhere. I can certainly think of an area that I knew

quite well where crime was reduced by a very effective if somewhat intrusive CCTV system but at the same time crime rates just down the road rather increased.

**Professor Norris:** There is evidence for both displacement and for the halo effect. Certainly from the study in Doncaster conducted by David Skint city centre crime did reduce but it spread to the outer lying townships and there was statistically significant evidence to that effect. There have also been arguments for which you will also find some statistical evidence that, if you put a system in a particular geographical area, it could have effects on the surrounding areas which do not have cameras. Overall, the main level of effect is actually not very much.

**Q51 Lord Morris of Aberavon:** Does it not give a perception of safety to people when there are CCTV cameras?

**Professor Norris:** If you look at the evidence from the Gill study which is the largest study conducted, a three/four-year study funded by the Home Office employing a large number of researchers, their conclusions were that it did not increase people's feelings of public safety.

**Q52 Lord Morris of Aberavon:** It is the perception of people that I am asking about.

**Professor Norris:** Your feeling of safety is a perception. It did not increase people's perception that they were safer. In a way, we can see that that has been recognised. The whole of the city centre warden movement to having in a sense a visible authoritative presence on the street that is not necessarily police is about responding to that public demand that what they want is people not machines and technology and it is people who make people feel secure rather than machines.

**Dr Murakami Wood:** I have carried out a great deal of work in Japan and it is a useful comparison in this case because Japan is a society traditionally regarded as having a high level of social trust and very low crime rates in comparison to western countries. What

I found from talking to people there, especially women – and CCTV is only now being introduced in public spaces with government support – is that, when they saw cameras, they felt less safe and not more safe because that made them think that the area was dangerous, that there was something they should watch out for. Whereas no cameras made them feel their normal level of trust in other people. It really depends on the level of social trust which you have in a society and I think that cameras are probably a mark of the decline in social trust and indeed may increase further that decline in social trust as we rely more and more on technology to replace and compensate for the decline in trust that exists overall in society.

**Q53 Chairman:** I have one final question on this before I ask Lord Smith to come in. Are you able to say what the evidence is of the effect of CCTV on detection?

**Professor Norris:** The simple answer to that is, “No, I cannot, not with any certainty”.

**Q54 Lord Smith of Clifton:** What do you see as the key adverse effects of state surveillance? Do they go beyond the deleterious effects on individual privacy?

**Professor Norris:** Yes. One needs to think about this mainly in terms of mass surveillance rather than individualised and targeted surveillance. There are four broad issues here. Firstly, there is the issue that mass surveillance promotes the view in a sense that everybody is untrustworthy. If we are gathering data on people all the time on the basis that they may do something wrong, this is promoting a view that as citizens we cannot be trusted, and I think that that is a general issue. A second problem is that once you are into a surveillance solution, it becomes in a sense expansionary to a huge degree. If you see that information is what you need to solve a problem but you do not quite know what that problem is and you do not know what future events you are going to be responding to, the temptation is to collect all information about all people, and that is in a sense partly the way that things have gone. If one thinks about the new criminal records system which will integrate the databases of all

police forces including all the intelligence files on 11 million people, I think it is 65 million records that will be integrated, all information comes to bear and then there is the idea that we have to join this all up. So, the information held in health fields, education fields and welfare fields all becomes part of the resource to solving a particular problem. The expansionary nature of a surveillance system is a problem if it does not have checks and brakes to it. The next point relates to what we said earlier. I think that there is an undue faith in technological solutions to the problem of crime, security and order. The best evidence is that order, crime and security are best promoted at a local face-to-face negotiated level. The best way for police to solve crime is if the public give them information freely. It is if the public trust the police that there is that flow. That is about a reciprocal relationship. One of the problems one has with reliance on technological solutions is that we can create a distance between police and public. We can see a police that actually see themselves as standing outside the community and coming down in a sense from the mountain to impose order rather than a police that are an integral part of that community who have to negotiate, sometimes with discretion and toleration, with various communities and individuals but, in that process of trade-off, what one does is build up trust and consent and consent is at the heart. I feel that the faith in technological solutions may actually lead to, in a sense, a shift from one of the fundamental principles of British policing. That would be my third point. My fourth and perhaps actually in a way the most serious issue is that, as one creates a mass surveillance system, as this personal information becomes more and more available, what we are seeing is the idea of risk assessments becoming more and more prevalent in various aspects of certainly criminal justice management but also within education and so forth, and the risk assessment provides the basis for pre-emptive intervention. I think that this is a really serious issue. The issue of course is that we normally talk about intervening with people in the criminal justice sense on the basis of individualised reasonable suspicion. Indeed, the PACE Codes of

Conduct actually say that you cannot stop and search someone merely on the basis of a category such as their race. You have to have a better reason than that. Where you collect information and you say that if an individual who in a sense shares the characteristics of other individuals who deviate in some way and therefore are seen as criminal or whatever, that gives us the right to intervene with them and their families with various social programmes, some of which may have punitive elements to them. This seems to change and challenge in some ways and I am not sure that I understand all the ways it does, but ideas of reasonable suspicion and the presumption of innocence, for instance. Something is going on here that I think represents a fundamental shift which our concepts have not quite caught up with. I think that is how I would see the main adverse effects, but again I am particularly thinking about the mass targeted.

**Q55 Lord Smith of Clifton:** I would like to press you on this and it seems to me that you began to allude to this. Are there some categories of individuals or social groups who are adversely affected more than others?

**Dr Murakami Wood:** First of all, the thing to say is that both ends of the social spectrum, the most wealthy and the worst off, are both subject to high levels of surveillance. There is a big difference. Those at the top end of society tend to get the protective and inclusive benefits of this. This is surveillance that is voluntarily entered into for protection and for social inclusion in volunteering for systems like the iris scanning at Amsterdam Airport to speed you through immigration. You get better security, gated communities and things like that. At the bottom end however, there is significant deleterious effects on people's lives and Clive will detail some of these.

**Professor Norris:** If you look at the studies done on the operation of CCTV – and I think this raises one question about all these systems – generally these systems have elements of discretion built into them. They are not just automatic systems following automated routines;

they involve people making choices. CCTV operatives have to make choices about who to target and the evidence is that they are most likely to target young males particularly if they are from ethnic minority communities. In terms of the way that that has an impact, actually it is not so much in the public sphere of the town centre, it is more in evidence in the private sphere of the shopping mall with what sorts of people tend to get excluded from those areas. It is not just that they get excluded for criminal infraction, they are getting excluded because youths in a shopping mall are hanging about and they are not shopping and they are asked to move on. If they suggest that they have a right to be there, they are told that they do not. It is private space, so maybe they do not have a right to be there. Then they are excluded. If they argue too much, they will be banned from the shopping centre and the cameras and the security officers will enforce that ban. So, there is a form of exclusion that can go on which tends to target particular social groups and not generally us, as it were. If I may take another example, we have introduced mandatory drug testing in prisons. One of the features of such systems which seem to me to make them at least have elements of fairness in them is that they are random and, when they are random, everyone has an equal chance of being subjected to them. Unfortunately, there is also a little bit that says if a prison officer thinks that you warrant drug testing, then you will get it. This introduces again a human discretionary element to it. What I do not know is the extent to which that may be based on discriminatory bases. We do not know the answer to that question. As soon as you do that, you have that potential. I think that the DNA Register is one where this is really very serious. The over-representation of black men in the DNA Register is a serious issue and cause for concern and part of that over-representation is because they are more likely to be arrested by the police and in some ways that over-representation in arrest statistics may represent an over-representation in certain forms of crime but, in other ways, what it represents, as we know that those people are more likely to be arrested without charge, more likely to be acquitted and so forth, is that

there is evidence that this is not just on the basis of good evidence. So, we have a system that is disproportionately including someone on a register which will affect their life chances in ways in the future which is based on forms of differentiation and I have suggested perhaps at times forms of discrimination.

**Q56 Lord Morris of Aberavon:** Am I getting the wrong impression? Is it that neither of you are keen on any form of surveillance or is that wrong? In your written evidence, you refer to “the emergence of a ‘safety state’ obsessed with security and stability, and increasingly favouring the precautionary surveillance of groups, categories and individuals ...” What are the main dangers of this kind of approach?

**Dr Murakami Wood:** First of all, I think that it is very important to stress that we would never say that surveillance itself is a bad thing. If you read our report which we wrote on the surveillance society for the Information Commissioner, we are quite clear that surveillance is often about the best intentions regarding care and indeed many of our functions in a welfare society would not be able to work without surveillance. Indeed, safety and security of the Realm are also assured by surveillance in many cases. We would like to make it quite clear in the record that we are not suggesting that all surveillance is wrong or that surveillance necessarily has negative effects and Clive will talk about what we mean when we talk about precautionary surveillance.

**Professor Norris:** Again, it seems to me that there is this problem of if one is gathering information pre-emptively on a citizenry on the basis that they might commit future crimes, one is widening and changing the nature of the contract. If you look at the document on transformational government, it is clear that what is envisaged is basically a merging of all the data held by government in various forms. Information sharing and taking down the silos are key elements of that report. One of the questions for me here is that we have a regulatory system that has been built up on the principle that you give information for a particular

purpose, but you give information in a context and it is to be used in that context. We now have a situation where it appears that what is emerging – and it is emerging – is that the context is merely governance, that you give information at one point of the system. So, as a child you have information recorded about you – I am not sure that you freely give it but it is certainly recorded of you and from you – and that can then become available at another point in the system, a criminal justice context for instance. This seems to be a change in the nature of how we have traditionally thought about information and about the extent to which people have the right to control information about themselves and how it is used. I think that that represents a significant shift. Does that answer your question?

**Q57 Lord Morris of Aberavon:** Up to a point only. You mentioned DNA testing. Presumably you would take an adverse view of the collating of information. You mentioned classes of people who will get on that register. What about the balance of advantage which might occur when people who have committed an offence 20 years ago are apprehended on the basis of information that happened to be stored? Would you put the ID card in the same category? Would you put the collating of health information, a study about which a large number of doctors are refusing to take part in, in the same category? Are they all in the same bag, as it were?

**Professor Norris:** No. In a sense, I think that the issue of the DNA register raises some very interesting questions. If we are as a society prepared to accept – and we seem to have been – that the police may arrest somebody, not charge them, take their DNA and store it on a register, then I am slightly concerned because actually I think that the issue becomes, if merely arrest is the criteria for being on the register, (1) it gives the police a perverse incentive to arrest people because I think there is advantage to the police for having the register, it has definitely to be shown to be ---

**Q58 Lord Morris of Aberavon:** An advantage to all of us maybe.

*Professor Norris:* But then I think the question becomes, if it is so advantageous, we should all be on the register. That is something that one might have to consider.

**Q59 Lord Morris of Aberavon:** Why not?

*Professor Norris:* I am not saying “Why not?” I think that is the debate to be had.

**Q60 Lord Morris of Aberavon:** What would be your view?

*Professor Norris:* My personal view is, given the unfairness that I think currently exists in the system, I would be prepared to sacrifice my particular bit of privacy in this to ensure fairness, but I suspect that there are others, intellectuals and academics, who would strongly disagree with that position.

**Q61 Lord Rowlands:** I am trying to establish whether you can define relevant information. For example, in his evidence, the Information Commissioner spoke about the whole business regarding the crime record and what is collected in there is irrelevant to the actual question about whether you can or cannot work with children. Is there any way in which we could devise a system where we could say, “That bureau has the right to relevant information and we define relevant information in the following way”?

*Professor Norris:* I do not know is the answer. One can see that that would be a response to this problem. One of the matters which comes into this is that security and crime control often do seem to trump all other issues. So, one of the questions would be, what would be the exceptions to the rule that stopped this? Where would you draw the line?

**Q62 Lord Rowlands:** For example, would the fact that I had nine points on my licence be relevant to whether or not I could work with children?

**Professor Norris:** It is interesting that you say that because I am someone who has to sign this for potential social workers and that is indeed an argument that gets had. I do not want to say how we resolve individual cases but certainly there are arguments on the committee which deals with these matters about whether it should or should not. Some people view that it should and some people view that it should not. My point is that it is never very easy to draw the line. We may think that a driving offence is seen as not being relevant. A driving offence that maybe severely injured a child would show a recklessness or could show a recklessness.

**Q63 Lord Rowlands:** That would be a criminal offence.

**Professor Norris:** Okay but being caught for speeding could have that effect and although it did not have in that particular case, it would be evidence that it might have. So, I think that points on the licence could be argued in that way.

**Q64 Baroness Quin:** Debates certainly here in Parliament often are framed in terms of talking about the balance between security and liberty. It was interesting that, in your written evidence, the Surveillance Studies Network evidence, it suggests that talk of balance between security and liberty is highly misleading because liberty is an integral component of what makes security for citizens and that, without liberty, there is no citizenship and there is only insecurity. Can you expand a little further on that for us.

**Dr Murakami Wood:** We put this in this way quite deliberately because there is this tendency to assume that the balance exists. What we are trying to say here first of all is that there are not equal quantities of this stuff on either side that you could take from one part and put in another part. We exist in a society of a kind of tacit social contract where we expect to be free and to have those freedoms protected and the main reason for security is to protect our rights to go about our daily business unhindered. Where that protection starts to remove those

freedoms themselves, I think that tacit contract is challenged and it is a tacit contract in this country because we have no fundamental constitutional protections in the sense that some other countries have a written constitution. So, it is particularly important in a country like Britain where a lot of the contact is tacit. If those things are challenged, we generate a sense of insecurity and that is very important. Those senses of insecurity are in fact in some ways all we are left with. This can, in an extreme form, mean that you lose any meaningful sense of citizenship because, if you have no belonging, all you are left with is a sense of security where the state is no longer guaranteeing those things which you regarded as being part of that tacit contract. What is left is a void. You have no sense of citizenship. This case, in an extreme case, lead to that complete absence of citizenship, and that is an extreme and we have not reached that point in Britain. The key questions here are first of all, what is security? What are you arguing is security? What we are arguing is security from the beginning is that sense of guarantees for our liberties. Also, it is important to say what is being secured and we are also arguing that it is vitally important to consider what is being secured by security. If what is being secured is ultimately just the state and what the state does, then, as far as I am concerned, that link with liberty is entirely lost. It becomes almost meaningless to talk about security if you are just securing the securors, if you are just securing the state. I think that it is vitally important and the reason why we put it in this way is that we are talking about securing liberties, not about playing off security and liberty. I know that that might sound like semantics, but I think that it is quite important because otherwise you allow certain things to be lost and the point is that there are some things that are always off the scales and they should not be included in any balance. We should not be putting everything in the balance. For example, I think that torture is always off the scales. Our American friends may disagree or some of them may disagree. Certainly, for us, I think that torture is always off the scales. You do not weigh up that particular item in a scale of security and liberty. I think that there

are several other things that we would – and many of us would probably have different views on this – say are off the scales. That is why I think it is important not to say that there is just this balance. There are things that are not to be balanced and not to be included.

**Lord Peston:** May I take us on to the enormous growth in surveillance in our society certainly over at the age group of most of the people in this room, we have gone from when we were young with no concept of surveillance at all. Those of us who lived in the war had identity cards; I have never forgiven my parents for losing mine but that is by the way, but that was about it and there was no such thing as surveillance. A lot of what we now have is economics driven. We did not have supermarkets and, if you get supermarkets, you get shoplifting and then you get surveillance and it is quite clear what the cause is. It is not a higher propensity for people to be criminals, it is the fact that you create an environment in which criminality, in this case shoplifting, becomes the sort of thing one does. To go back to your class point, all my life middle classes have never regarded taking things through Customs illegally as a crime; it was regarded as a game and you always took more than you should through Customs.

**Baroness O'Cathain:** I certainly did not.

**Q65 Lord Peston:** So, there is a real class point here as well as everything else. I did not! Quite the contrary. Not being middle class, I have always been terribly frightened of the police and that goes back to another one of your points. Is the rise of surveillance very much economics driven is one question, and the other one is, is it supply side driven, namely firms make the relevant kind of equipment and then naturally they want to sell it and, for all I know, although I actually favour ID cards but in a much more limited sense that the Government are going for, there may a great industry ID lobby that intends to make billions out of ID cards?

**Professor Norris:** I would argue with you in that I do not know that there has been, in the way you are thinking of, such a growth in surveillance. I think that there has been a change in

surveillance. When I used to come to Westminster to school – I went to Westminster City School in the 1970s – I used to get on a train. When I got on to the station, there was a platform guard and, when I got on to a train, there was also an end guard on the train, and that was whenever the station was open. The last time when I went to that particular station at 8.00 in the evening, there seemed to be no-one there at all. There was a help point which told me that I could press a button and that someone would answer and that I was being watched by CCTV. We have changed the nature of surveillance: conciergeship, face-to-face knowledge about people has changed. You are right in the sense that we did not necessarily see it as surveillance then. I think it is only when we have lost it that we understand that this had a control function often never put into practice because it was not needed because it was there. I think that is one thing. If you want to ask why there has been such a growth in surveillance in this country, one reason is because there has been little to stop it. The point about the constitution is, if you take, say, Germany, in Germany within the constitution, there are words to the effect that people have the right to self-determination and self-autonomy. One of the things that means is that you can appeal to the constitution about the presence of a camera because a camera is seen as reducing your ability to act autonomously because – and this is the way the Germans would argue – knowing that someone is watching you in a public space influences your behaviour and you are less free. That does not mean that you cannot have cameras in Germany. What it means is that you have to make a special plea as to why the camera is justified in that circumstance. So, it creates a brake. In Britain, in terms of cameras at least, there was no brake to be applied. There was no privacy law. There was no law to prevent cameras being put up. There was nothing to stop it and we had no higher appeal: we could not appeal to a privacy law because it was not there; we could not appeal to a constitutional principle like the Germans or maybe even the Americans or other states could. I think that that is very important. I think that, at a more general level as well, in

continental Europe, surveillance is viewed at the public level with rather more suspicion and as something that is potentially dangerous. The reason for that is the experience of in the German state of being taken over by a fascist regime and then, in European countries, by being invaded and understanding what actually surveillance could mean for particular sections of the population, and this notion that a state does not always act in the interests of its people. When it is being invaded, the occupying state clearly has mal-intention. I think that there is a danger in Britain that we see and perhaps with good regard that our Government are generally benign and have been. On the continent, they know that their governments have not necessarily been so benign. I think that we do have to recognise that the future is an unknown quantity. We do not know what 50 years will bring. Therefore, we need to think about, if we are setting up systems, what will the consequences be if, in two or three generations, our rulers are not so benign?

**Chairman:** I repeat my appeal for reasonable brevity.

**Q66 Lord Lyell of Markyate:** I want to talk about regulation and the improvement of regulatory policy – we do not have much regulation at the moment – about Smartdust, which I remember you told us about, and about Google Earth. As I understand it, you could be sitting in your garden and you could be watched by everybody who had access to Google Earth. Exactly how accurate it is at the moment we do not know, but I think we can anticipate that it will become or could become extraordinarily accurate. Smartdust could be scattered around the dining room table and all our conversation could be listened to. To what extent do you think those things should be regulated?

**Dr Murakami Wood:** This is at the heart of the matter here and I think that it is absolutely essential that we develop some ways of regulating these kinds of technologies. I would like to say how Google Earth is at the moment. It usually relies on stored satellite images and therefore on the whole is not conceived as a live image in many countries. In America,

I think that they can produce relatively swift images but certainly not in most of the world yet, but you are right that this is just a technical impediment which will be overcome. Things like Smartdust do present an entirely new challenge because we are not looking at traditional forms of surveillance that can be seen. We are talking about all kinds of new technologies that present new challenges. Here, what we need is for policy to be able to deal with things that they have not conceived of previously in the past and the problem at the moment – and it goes back to your question about where this is coming from – is that the other driver of surveillance in this country is indeed the political economics driver, the driver of industry. Industries are producing more and more highly advanced technologies. That seemed to come as a complete package; it seemed to be a solution to social problems in a nice, neat technological bundle which is very attractive to policy makers. Easy solutions are very attractive. The problem is that the policy makers themselves – and that includes all of us here, the academics who study them even in social terms and the bureaucrats involved – usually lag way behind the technological development in terms of their ability to understand even how the technology itself works as advertised let alone how it works inside, inside the black box. If I asked any of you to tell me how an algorithm works for facial recognition, probably even those of you who had technical backgrounds might struggle and I study these things and I struggle sometimes to understand how a few lines of code can create certain kinds of effects within a piece of software. We need some very new kinds of regulations and this requires detailed technical knowledge and it requires somebody, a regulator or a regulatory body, to be able to say that this is or is not acceptable, not just an advisory committee but somebody to say, “No, this is not acceptable and we should not employ this technology”. I think that there is a danger of us at the moment, especially in Government faced with the dangers of terrorism of crime, to say, “This technology looks like the silver bullet, it looks like the one that will solve the problem” and not consider what the bad effects

might be and almost never to say, “No, that is a step too far” or “We do not want that” when presented with something that seems to solve a problem.

**Q67 Viscount Bledisloe:** In your paragraph 4.2.5, you call for a new and comprehensive Information Act to create the basis for the information relationship between the state and the citizen. What would be the principal components of such an Act and can you give us examples of statutes in other countries which contain these components?

**Dr Murakami Wood:** We are asking here for two things. First of all, to bring together the piecemeal and existing legislation that we have had in this country for a very long time. The British way in many ways has always been to do things gradually and introduce things bit by bit and this works in a context where things change slowly. We are looking in a context now where technological change is extremely rapid. For example, the Data Protection Act is conceived on the basis of an understanding of the computer that derives from the 1970s. Even though it was introduced in the 1990s, its understanding of computing is based on a much earlier period of understanding of what computers could do. We need to move ahead of the game. We need to bring together these various pieces of legislation that already exist first of all and understand their relationship. For example, the fact that freedom of information should be working in a reciprocal way with things that deal with surveillance, they should not be entirely separate domains, they should be connected. The first thing to do is bring together those existing pieces of legislation, start to connect them, start to see where the holes are, to fill those holes and then to go further and to actually start to think in terms of the future about what might occur and how we might legislate for things that are now being developed or will be developed. Most importantly of all, this is about setting a framework for how Government and citizens should exist in the information society. We still have not really done this. Japan started to do this in the 1980s; they started to consider these issues and never really went that far but Japan started to do that. We never did. In the absence of

conventionally understood constitutions, I think that this stage is a good time to take stock and to establish these new kinds of fundamental relationships between citizens and Government in an information society. So, understanding the information rights of citizens and understanding what information means to people.

**Professor Norris:** The other thing here is that if we say that personal data primarily should belong to the person in whom it originated, then what is the relationship between that person and the state's holding of it and how can that person audit the information that the states holds on them? I think that this becomes absolutely critical when that information is obtained without somebody's consent, that is without their voluntary consent. For instance, the DNA register is not a voluntary consent piece; you are coerced into giving your DNA for that. Similarly, CCTV cameras that record your number plates – and we are moving to a position now where the police will hold 50 million records of vehicle movements per day – is non-consensual. We have not consented to this act. I think as a citizen that, if the state is holding my personal information, the state should have a responsibility for demonstrating to me that it is accurate, that it is fair and that they have collected this information. How one manages that is problematic but I think that it is implied. These are things that we think an Information Act would have to start to grapple with and have some fundamental principles involved. However, neither of us are legislators and we would not say that we know that answer.

**Q68 Lord Rowlands:** Following on that, if a bill came forward on any new Information Act, what would you say about the Information Commissioner's powers? You call him an effective but shackled regulator. How would you unshackle him or how might he be unshackled?

**Dr Murakami Wood:** What we meant by this first of all is that we regard the current Information Commissioner as being an extremely active and effective regulator who has gone in some ways way beyond what he needed to do and has indeed sparked this whole debate in

the first place. He is shackled in the sense that his powers are limited and indeed the powers of his office are limited. We would first of all see a requirement for a huge increase in resources for the Information Commissioner's Office. We would see the Information Commissioner as being the primary regulator of any kind of new information and in fact not just to be provided with the powers of inspection and prosecution that he would need for the state but also for private companies. I think that this is absolutely vital; we are talking about these vast new conglomerates of information like Google, Tesco Clubcard and so on. These need to be subject to inspection as much as the state and the state certainly does. Also, there should be not just a reactive set of powers but we would also like to see an active responsibility for the Information Commissioner to be not just a statutory consultee as is suggested here, but to have the right of veto over new technological developments. What I mean by that is that in several countries – and I am thinking of Canada here in particular – Privacy Commissioners are able to specify where or if certain kinds of technologies or systems are implemented. If we are going to have the technological expertise to assess these new things, these need to be vested in an authority which is trusted and which has a statutory function and I think that the Information Commissioner's Office would indeed be the place to put these functions.

**Q69 Lord Rowlands:** It sounds like a large, new empire in some ways. Some of them would become a sort of look-alike from ...

**Dr Murakami Wood:** We have, for example, the National Audit Office when it comes to financial issues like this which is indeed a very large organisation and it has large responsibilities. I would suggest that in fact information is as important as finances for government and for governance and the relationships between citizens and government in the future and therefore it should be taken as seriously, funded as well and regarded with the same degree of statutory authority.

**Q70 Baroness O'Cathain:** How worried do you think the general public is about surveillance? How satisfactory is the public knowledge of surveillance or do they actually want to know about it because most people now exchange all this information on Facebook and the Internet and bringing the National Audit Office into it when you ... It is quite a different subject. You could not control something that is blowing around in the ether throughout the world.

**Professor Norris:** I think that we have a serious job in educating our children about the dangers of some of their practices. Because children are doing this does not mean that it does not bring dangers. I have a son who uses Facebook and so forth and it clearly worries me about the level of personal information that can be obtained. I do not think that just because they do it that we should say that it is okay because I am not convinced that it is and I think that we have a duty in some senses to create structures to protect youth from such follies.

**Q71 Baroness O'Cathain:** Let me pursue that. What sort of structures could protect people, because of the very nature of Facebook and the Internet and all this area, and dating agencies on the Internet?

**Professor Norris:** I think a growing awareness of the danger of allowing your personal information to circulate freely. There are ways of dealing with this.

**Q72 Baroness O'Cathain:** How?

**Professor Norris:** For instance, the conversation that I had with my son last week was to suggest that he did not disclose his real date of birth, that he lied on his Facebook. You can do that.

**Q73 Chairman:** Dr Murakami Wood, would you like to come in for the final word.

**Dr Murakami Wood:** What is important to remember with these kinds of systems is that they have only been around for three or four years. We are talking about incredibly new phenomena and these people are being very naïve and it is not just children. There was the case recently of a senior police officer who was also giving away large amounts of personal information.

**Professor Norris:** He is the Head of the Security Service.

**Dr Murakami Wood:** He was giving away plenty of personal information on his social networking site. A number of people are very naïve about these kind of systems and we have to remember that this will not be the final condition, if there is such a thing, of these systems in the future and that we will learn and in fact we will have to learn very soon. If you combine this with the issues we have seen in the last couple of weeks of the loss of 25/26 million people's data by Revenue and Customs, our naivety about the amount of information and how it is used out there has to come to an end very soon and it will do. I think that we are seeing the emergence slowly of what we are calling personal information economies where people start to take more charge of their person information, to realise its value and to take steps to protect it. We are seeing the rise of people like information brokers who will look after your personal data for you and create a better profile for you and people using things like credit referencing agencies to start to manipulate positively their data image on the web. I think that we will see a growth of knowledge. This will not be the final state but it is a very dangerous time and I think this is why we need this new set of legislation and why we need to take some responsibility when acting at this dangerous time.

**Chairman:** Thank you very much. Professor Norris and Dr Murakami Wood, may I thank you both very much on behalf of the Committee for being with us and for your evidence.

## Memorandum submitted by Professor Graham Greenleaf

### Examination of Witness

Witness: **Professor Graham Greenleaf**, Professor of Law, University of New South Wales, Australia, examined.

**Q74 Chairman:** Professor Greenleaf, good morning and thank you very much indeed for being with us.

**Professor Greenleaf:** Thank you very much for the invitation to appear before the Committee.

**Q75 Lord Morris of Aberavon:** I would like some comparison of surveillance in different countries. You have experience in your native Australia and other countries as well. How does the degree and nature of surveillance in our country compare with that of other countries? Are we much more restrictive than others or does it vary?

**Professor Greenleaf:** It varies. I cannot purport to be an expert on the details of surveillance in this country; I have picked up what information I can for comparative purposes and I will try to make some comments in comparison with, say, Australia and with Hong Kong which are perhaps the two places with which I am most familiar. In relation to Australia, I have, with the assistance of my colleagues, anticipating that the Committee would like some information about this, prepared some background information about the nitty-gritty of surveillance practices in Australia. I would like to hand that to the Committee. I would like to comment in summary. Australia and the UK could both be put at the more advanced end on the spectrum of surveillance orientated societies, but there are a number of differences between the two and overall I would say that the United Kingdom is probably further down the track of more intensive surveillance than Australia or at least going in that direction.

I would like to pick up a couple of different indicia. There seems to be much more CCTV surveillance in the UK than in Australia. Whether the estimates of 4.2 million cameras are correct or just in the right ball park I do not know, but the Australian figures in the documents I have suggest numbers more in the tens of thousands for the largest capital cities. So, at most, you are going to be looking at only a fraction of the UK numbers and they are mainly, from my knowledge, orientated to transport systems and large crowd locations with some private sector use in large supermarkets and the like. In relation to the ID card system that has been proposed or is in the process of being implemented in the UK, from what I know of it, this vast aggregation of data with very wide and uncertain purposes in both the public sector and the private sector goes far beyond any other systems with which I am familiar and seems to almost constitute the surveillance society in itself. You may be aware that the Australian Government were proposing to introduce what they call an access card for health and welfare benefits of which I have been a critic for some time. That is now not going to happen due to the change of Government in Australia in November 2007. So, on these particular indicia, Australia is going to be in the future a far less intensive surveillance society than the UK. Other factors such as the children's database, the NHS patient database with its very wide accesses and the DNA database, from what I know of them, the cumulative effect of these is far, far greater in the UK than the equivalents that do exist to some extent in Australia. If I may turn to the private sector, I think the big difference is that there are very few barriers in the UK to data sharing between different sub-sectors of the private sector, say between the credit industry, the insurance industry and the direct marketing industry. In Australia, because of legislation introduced in the early 1990s, information in the credit reporting sector is in effect siloed off from the rest of the private sector and that has made an enormous difference to developments in Australia compared, say, to the UK or the USA. So, quite a different picture. On the other hand, there may at the present perhaps be less

government data matching at the moment in the UK than in Australia but, from what I have seen of recent announcements and committees looking at this, it seems as though the UK is catching up fast. One of the areas where there is very intensive surveillance in Australia is anti-money laundering where vast amounts of data are being sucked in by our money laundering agency from all sorts of cash dealers and any organisations involved in finance in the private sector. I suspect that there is more of that in Australia than there is here. May I mention something about Hong Kong by way of comparison as well?

**Q76 Chairman:** Yes.

**Professor Greenleaf:** I was a Distinguished Visiting Professor at the University of Hong Kong for a couple of years and that is why I have some knowledge about Hong Kong. I think that it is an interesting comparison, it having been a UK colony only a decade ago and now part of the People's Republic of China. Although Hong Kong was one of the first countries to introduce a multi-functional chip based Smart ID card, in fact its non-immigration uses are at present quite minor. The main criticisms that I and others have levelled at it is the potential for function creep in the future that has been built in. However, at present, it is not anything remotely like the UK system that is being developed. Data matching is quite limited in Hong Kong and must be approved by the Privacy Commissioner. I think that there is relatively little CCTV surveillance except in a few select areas of downtown entertainment areas of Hong Kong island, and not a whole lot more other than that. Transport surveillance is quite limited compared to what is being used. The Oyster Card here I gather is quite extensively used for police surveillance now. The Octopus Card is an anonymous smart card in Hong Kong and has very limited possible uses for surveillance. Telecommunication surveillance is also relatively limited. They have a new Interception Commissioner but the numbers involved are not very large. You can do things like get anonymous SIM cards for mobile

phones by cash payments. Anonymous mobile phones is quite surprising in a jurisdiction which is part of the People's Republic of China.

**Q77 Lord Woolf:** You have already covered some of the matters that I was going to ask you about particularly because you have made a comparison between this country and Australia and then Hong Kong and of course a comparison between Australia and Hong Kong very briefly in what you have said. Having done so, do you think that part of the problem here is that our regulation at the present time is very piecemeal?

**Professor Greenleaf:** Yes, I do think that is part of the problem and this is not a problem that is limited to the UK by any means. Over the last 30 years, we have had the development at an international level of information privacy principles but there has been very little systematic development in the rest of the package, if we can call it that, of privacy principles, plus principles governing surveillance as such. These would make distinctions between overt surveillance and covert surveillance and what are the rules for each and whether there are different rules for workplace surveillance compared to open places and the like. Also, there are really no systematic sets of rules for intrusions of various types. I think that that leads to a lack of real rules in those latter areas which contributes to the proliferation of things like CCTV. It also means that neither Information Commissioners nor the general public nor the Parliament are able to get an overall grasp of what is the overall surveillance picture in our society and how these things are knitting together. We talk about the boiling frog but we do not really have much idea at what temperature from one year to the next the frog has reached. Yes, there is piecemeal regulation.

**Q78 Lord Woolf:** What is the answer to that? What is the solution you would like to see? Is that in turn piecemeal or is it one overriding form of protection?

**Professor Greenleaf:** I do not know that there is necessarily one answer to that. I think that you could have a general piece of privacy legislation which contains sets of principles for these various areas and maybe you could have one commissioner administering that but, in this country, I understand that you have commissioners for surveillance and commissioners for telecommunications interception as well as the Information Privacy Commissioner, as I will call him. That may still be a sensible model but it would be good if they were all working to one principle based set of privacy principles, even though they may administer parts of them differently. Picking up on the Information Commissioner's evidence last week, one thing that he did not say was that it would be good to have an annual "state of surveillance" report, that simply set out the facts on an annual basis of where each different type of surveillance had reached over the last 12 months and how they were now interconnected. That would enable Parliament, Government and everyone else to reach better policy decisions.

**Q79 Lord Woolf:** I think that there is the problem that can arise from what we have connected. We have had a very recent example of the problems of Revenue and Customs, one might almost say fiasco, with regard to the loss of information. Do you think that there are any lessons to be learned from that?

**Professor Greenleaf:** Yes, I think that there are a number of very serious lessons, particularly because that is what the future is going to comprise, in my view, if things are not changed. This is not going to be a one-off event. Some of the lessons that need to be learned are first that I think there has to be a serious acceptance of only collecting personal data where it really is necessary for organisations to collect it and not collecting it on some rainy day principle that it might come in handy some time in the future. I think that taking minimum necessary collection seriously has to be the starting point. In Australia, one additional principle that we have that is not found in the Directive or elsewhere is called the anonymity principle which

says that organisations must provide services to individuals on an anonymous basis where it is feasible and lawful to do so. Our Law Reform Commission is currently proposing that that be extended to include pseudonymity as well so as to provide an additional level of protection against unwarranted disclosure of information. One other essential starting point for this is to get the acceptance of privacy as a value correctly included in our privacy laws. For me, what this means is essentially that the onus of justification of intrusion in any way into a person's privacy has to be on those who are proposing to do it, whether it be government, private sector or whatever. Basically, I think that is what is at the bottom of the German Constitutional Court's "informational self-determination" decision. They were not making privacy any sort of absolute right but they were making it very clear in the German context that every intrusion into privacy had to be justified up front in terms of alternative social benefits. Once you get that sort of starting point, I think that you can be on the right track and I think that that is a constitutional principle and a good reason for this Committee to be looking at this issue. That really goes to the relationship between the individual and the state.

**Q80 Lord Lyell of Markyate:** That leads very well onto Article 8 of the European Convention on Human Rights which gives everybody the entitlement to respect to their private and family life and that seems to come pretty close to what you are saying and might be built on. Bearing in mind the very rapid change in technology and the ability of those involved in surveillance or data collection to be much more intrusive than they are today, how do you think that our regulators should respond? Do they have the necessary powers and resources?

**Professor Greenleaf:** No, I do not think that they have either here or in most other countries although, if you pick and choose from the best of what various other countries offer, you can usually anywhere come up with a good set of improvements. I have already mentioned that I think that the Information Commissioner should have a role in producing an annual report

on surveillance. When he gave evidence to this Committee, he mentioned that it would be good if he could help increase the effectiveness of parliamentary scrutiny by having a better ability to warn Parliament without having to be invited even to answer questions and the like. I would suggest going further than that and to give the Information Commissioner a statutory obligation to warn Parliament of any significant privacy dangers that he perceives in legislation or regulation. So, draw the line at “significant” so that he does not have to report every minor thing. In that way, he avoids having to justify why he intervened on a particular issue if he has a statutory obligation to do so and he cannot really be seen to be playing any partisan games in coming in on particular issues if that is his obligation. I think that it would be useful to give him that obligation and then it would be his responsibility if he did not do it properly. In his evidence, the Commissioner said that he may not have shouted loud enough about the DNA database. There would be some comeback against him for not shouting loud enough about the DNA database to Parliament. May I mention a couple of other possible things or do you want me to stop?

**Q81 Chairman:** Very briefly because we have a great deal of material to cover in the next ten minutes.

*Professor Greenleaf:* Then perhaps it is more sensible for us to go on with further questions.

**Q82 Viscount Bledisloe:** You have very largely answered my question already when you were answering the questions of Lord Woolf. Am I right in understanding from you that you think there should be a comprehensive single statute on the right to privacy and that the onus should be on the person wishing to use your information or collect your information to justify that within defined grounds?

*Professor Greenleaf:* Yes, that is right, that is what I think. You could do that by not having just one statute but by having, say, a surveillance practices statute which effectively locked in

with the information and privacy statute, but it might be more sensible to put it all in the one. I would like to say one further thing on that. On the question of privacy torts, I do not think that, in light of the case law in this country, there is any likelihood that a privacy tort will be developed by the courts. Although there are some developments in the area of breach of confidence that are useful, they will not cover other areas like surveillance. However, statutory tort provisions like those suggested by the Hong Kong Law Reform Commission in a very detailed report have been recommended by the Australian Law Reform Commission in its draft report and considered by the New South Wales Law Reform Commission. They could well just be included in an overall privacy statute.

**Q83 Baroness O'Cathain:** What are the limitations upon the exercise of individuals' consent to data collection and further processing and are they insuperable?

**Professor Greenleaf:** I think that consent is an instrument of limited value in privacy statutes and it has been somewhat abused by consent not being clearly enough defined. It easily becomes a question whether there is implied consent in circumstances where there is hardly any consent at all. Where genuine fully informed consent (where the individual really has the alternative to consent or not consent without being denied valuable services) is possible, of course it is one of the reasons that do justify what would otherwise be interferences with privacy. But where that fully genuine consent does not exist, it is better just to accept that the requirements should be first that there is justification for the interference and then notice that the interference is going to take place. I know that is a long way round to answer your question but what I am saying is that I think we should put consent in its proper place and not exaggerate its relevance to privacy laws.

**Q84 Viscount Bledisloe:** Are you really saying that every time one is required to fill in a form compulsorily, there should be a box at the bottom saying, “Do you consent to this being given to other departments” or “given to other people”?

**Professor Greenleaf:** No. What I am saying is that if you really do not have any choice but to consent, then let us not go through the charade of asking people to consent.

**Q85 Viscount Bledisloe:** Surely you always do. You have no choice but to fill in the form, but surely you should be given a choice as to whether it is then disseminated.

**Professor Greenleaf:** Yes, you should be given that choice unless there are very serious other social interests that mean that the information must be disseminated to others. Where those serious reasons exist and you are not going to get some social service or you are not going to get some private sector benefit unless you tick that box, then we should not be calling that consent.

**Q86 Lord Rowlands:** Is there sufficient international coordination in this whole field and is it possible or valuable to establish some kind of international standards of personal data practices and surveillance?

**Professor Greenleaf:** I do not think there is sufficient international coordination as yet. The shining example of good international coordination is the Article 29 Committee under the EU Directive where the Data Protection Commissioners of Europe have genuinely provided policy leadership for the whole of Europe. In the Asia Pacific region, our Privacy Commissioners, although they have a collective Asia Pacific Privacy Association, have not done that. They have not taken a policy development or a warning role at all, partly because there is no glue like the Directive to hold those countries’ policies together. As a result, at a global level, commissioners are still rather hamstrung on reaching agreement about policy issues and have been very mild in their collective statements. To move on to the second part

of your question, I think that there is still a very serious need to establish a standard for exports of personal data between countries. That is still a pressing issue and, as yet, the policy instruments that have been tried have not succeeded in delivering that. The adequacy decisions under the EU Directive which, if properly handled, might have forced an international standard on the world, if you like, have not done that because the EU has lost credibility by caving into the USA and also because ---

**Q87 Lord Rowlands:** How did they cave in?

**Professor Greenleaf:** They approved a proposal by the USA for its “safe harbour” proposals which, in most people’s opinion, did not satisfy the adequacy tests under the EU Directive. However, for political reasons, the EU decided to let the USA go and the adequacy test lost a lot of its credibility as a result. They have also failed to reach decisions even about the most obvious jurisdictions to which they could have granted an adequacy finding like New Zealand or Hong Kong. The whole process, if it keeps going, will take to about the year 2099 before they get through most of the world.

**Q88 Lord Rowlands:** I am not sure that I understand what adequacy means.

**Professor Greenleaf:** For the purposes of EU countries under the Directive wishing to export personal data to countries outside the EU, it means that exports must be to a country that provides “adequate” data protection standards. But the EU Commission and the Council of Ministers make the decision – I should not go into EU Government matters – as to which countries meet that adequacy standard. So far they have only made a handful of decisions and the process is just bogged down and been discredited. The APEC Privacy Framework in my part of the world has contributed to undermining a search for a global standard. No UN conventions are really possible. The International Standards Organisation is not the right place to start for global policy. Surprisingly, I think that the only credible contender for the

development of a global policy standard is to follow the direction or the lead of the Council of Europe Cybercrime Convention and consider using the Council of Europe Convention concerning data protection (Convention 108) as a way of bringing non-European countries into what could become a global standard. There are provisions in the Council of Europe Convention allowing this which have never been utilised. The Council of Europe can invite countries like, say, New Zealand to become a party to that convention. It is the only agreement I can see that could possibly turn into a global privacy standard which would not be too high a standard or too low a standard but somewhere in the middle.

**Chairman:** Professor Greenleaf, thank you very much indeed for being with us and thank you very much for your evidence.