DEPARTMENT OF HOMELAND SECURITY

PRIVACY OFFICE

PUBLIC WORKSHOP CCTV: DEVELOPING PRIVACY BEST PRACTICES

MONDAY, DECEMBER 17, 2007

Hilton Arlington

Gallery Ballroom

950 North Stafford Street

Arlington, VA 22203

PANEL ON INTERNATIONAL PERSPETIVES

MS. BALLARD: My name is Shannon Ballard. My colleague Lauren Saadat and I are associate directors for international privacy policy in DHS's Privacy Office. We want to welcome you back. We'd like to note that the bios are in your folders, the handouts, and the presentations that are being presented this morning will also be on the Web site after the conference. I'd like to briefly introduce our panelists in the order that they will speak.

To my right is Mr. Phil Jones, who is the assistant commissioner and director of data protection practice of the U.K. Information Commissioner's Office. Mr. Ken Anderson is from the Ontario, Canada, Information Privacy Commissioner's Office. He is also the assistant commissioner. Then, to my left, we have Clive Norris, who is a professor of sociology of the University of Sheffield in the United Kingdom, and also deputy director of the Center for Criminological Research. And Mr. Wade Deisman, who's the director of National Security Working Group and professor in the department of criminology at the University of Ottawa. So, we're going to start with the regulators first, and then we will have the professors begin their discussion. We'll open questions, around noon, from the audience members, and we'll ask you to queue up at that time. So, if we can start with Assistant Commissioner Jones, thank you.

MR. JONES: Good morning. First of all, I should say that I have a slight embarrassment at being invited here, because I am well aware that that's because the U.K. is internationally recognized as the CCTV capital of the world.

[Laughter.]

MR. JONES: And certainly, to some of our European data-protection colleagues, they do look rather askance at us because of that. What I do want to do, though, is just spell out exactly how we operate in this area, and I'll try and give you a warts-and-all picture so that I don't try and gloss over things and make them sound better than they actually are.

A couple of points about the office that I work for. The Information Commissioner's Office is the independent data-protection supervisory authority. We enforce data-protection law. Effectively, that means that everything that organizations do that involves personal information, that they hold that for a business purpose, then our act will cover that, and we're responsible for providing advice to organizations on what they can and can't do with the information they collect, and how they should collect it. This immediately gives away the fact that something I want to stress is that giving advice on CCTV is but one of many things that our office does, because, as I say, we have to provide advice on the way that the legislation applies across the whole of the U.K. economy. That means that I'm not the technical expert, and, certainly in our guidance, we don't aim to have the degree of technical expertise that you've seen on the first panel. Rather, what we try to do is to point out the sorts of issues, the sorts of key considerations that those with greater technical expertise need to take into account.

I do think I should just stop, briefly, to mention a major conference that we organized in the -- for the data-protection and privacy community in London 2006, just over a year ago. What we did there was, we looked at the surveillance society. We weren't looking simply at CCTV, though a lot of people immediately think of CCTV. But our broad concern was the way that organizations, both public authorities and private organizations, are building up ever-bigger dossiers of information about us, and it was our view that there needed to be greater attention given to this so that we could seek to strike an appropriate balance between the needs of the State, the needs of businesses, the needs of organizations, and individual privacy.

Very thankfully, it was clearly a slow news time last November in London, and our conference got a great deal of attention, and it's actually resulted in several government committees in U.K. picking up this report and looking at it, and paying a lot of attention to it. So, it's one of those times when everything went right for us. One of the things we have done, as a consequence, is produce -- which we've launched very recently -- a privacy impact assessment tool. Certainly, I'm aware that there are other jurisdictions, certainly here in the U.S., but Canada, New Zealand, Australia have had these for considerable amounts of time, it's pretty new to Europe. And, thankfully, just showing what serendipity does, shortly

before we were launching this tool, the U.K. tax authorities managed to lose disks which had the details of 25 million people who were getting child benefit, and those disks included a great deal of information about private bank accounts. When I say that it's serendipity, this has certainly focused the attention in U.K. on information security, data minimization, all these sorts of issues. And, as I said, this was really a great piece of luck for us.

Moving on, the legal framework in U.K. is the U.K. Human Rights Act. The reason I mention that is, it incorporates European Convention on Human Rights, and, therefore, it writes in the right to respect for private life. We think, in the context of CCTV, that's important. I've already mentioned the U.K. Data Protection Act, which is based on a European directive, and the CCTV Code of Practice that we produced. The U.K. Data Protection Act has eight information principles. They're the fairly obvious ones that you think about. They involve adequate data, accurate data, not keeping data for longer than necessity, and, in particular, perhaps given the HMRC debacle with the disks, keeping that information secure.

In the late 1990s, we decided that it was about time that we produced a code of practice on surveillance. There were two or three reasons for this. In the '90s, CCTV schemes in U.K. proliferated. There was a great deal of public money given towards these schemes, and they did take off. There was a concern about the lack of regulation, and, due to a change in the law brought about by a new data- protection law in U.K., it meant that we had jurisdiction in a way that we hadn't before. What I want to do now is just run through a few of the key elements in that code. I will be fairly brief, because many of these things have been touched upon earlier.

But one of the key issues is who's -- what's the scheme trying to do? Is it appropriate to use CCTV? And who's actually legally responsible for this? And who has day-to-day responsibility? This is particularly relevant in the U.K. experience, where a lot of CCTV was set up, partly with local government involvement, but with a number of other organizations contributing and having access, including the police. In these sorts of partnership schemes, it's particularly important that there's clarity about who does what and who's got legal responsibility. We've already touched upon siting of cameras. Key issues here are making sure that, particularly when you're in a town center, a town center, it's perfectly reasonable to monitor streets, but if there are private housing there, private gardens, there's a need to ensure, as far as possible, that the cameras don't intrude on the private space of citizens.

The other point that I want to emphasize, and it's something that, in our guidance, we've always put a great deal of emphasis on, and that's signs. It's the idea of transparency, the idea of letting citizens know what's going on, what organization's responsible, what the purpose of the scheme is, and giving contact details for organized -- so that if individuals want to find out more about what's going on, they can do so. Clearly, there are also issues relating to the quality of the images. Several of these have been touched upon already. It's to do with the proper installation, proper management of the recording media, accuracy over

whether a date and time stamping, and I think this is an important point -- that proper attention is paid to maintenance. In the U.K., there was a lot of money that was given to the initial setting up of schemes. There was far less attention given to the maintenance of schemes. We actually have an ad hoc collection of schemes of fairly dubious, fairly varied quality, and there have been some estimates suggesting that something like 80 percent of the schemes capture images which are really not that useful at identifying people. With my private/data-protection hat on, that sounds quite good; as a citizen and a taxpayer, it doesn't sound so good. And also, the introducing of automatic recognition systems, making sure that the image is adequate, and also having human verification to make sure that there hasn't been a misidentification.

Moving on to process of the images, important issues there to do with retention. We've talked about that already. There's been a considerable amount of emphasis on training. Again, that's something that we think's important. Restricting access to images, ensuring that there is -- those -- when information is being viewed on monitors, this is done in a private way, and there's a limit to who can actually see those. And also, and quite important, that there should be very clear and well-documented handling procedures. Important, too, to ensure that there are clear rules regarding access and disclosure of images to third parties. Our guidance suggests that there may well be a need to disclose, in particular circumstances, to law enforcement agencies, prosecution agencies, relevant legal representatives. An important point here, to the media, but only where necessary for public assistance with a criminal incident. We don't actually think that, ordinarily, recordings from CCTV cameras should be used as some form of salacious entertainment of people who might be behaving badly or embarrassingly in a town center. There was a very important case, which I haven't got time to go into, of images of a man who appeared to be trying to commit suicide being given a fairly wide public airing. In our view, that was really quite wrong.

Moving on, images, therefore, not to be routinely broadcast. Again, that's to do with ensuring that there's a proper appreciation of the need to protect privacy as much as possible. Where information has to be made more widely available, then the blurring of images. We've touched upon that. And one of the other key points in our guidance is that those organizations that provide specialist services -- because in a lot of the smaller applications in U.K., they have to get in specialist contractors to manage the actual system -- there's a real need to make sure that those organizations are properly checked, proper guarantees, et cetera.

Under U.K. data-protection law, individuals whose images are captured on CCTV have a right of access to those images, so it's important that staff are aware of this and know how to handle such requests. And also, there's a -- will be a need, in certain circumstances, to make decisions on whether or not disclosing unblurred images of third parties who also happen to

be in the picture -- whether that is warranted or not. In some circumstances, it will be; in others, it won't.

Moving on, we think there shall be very active management of such schemes. We do think there should be complaints procedures, and we do think that there's a real need to be seen to take this seriously. Now, our original code was published in 2000. We decided, fairly recently, we needed to revise the code, partly because CCTV surveillance has grown hugely, partly because technology has moved on, but partly, in any case, because we wanted to take account of experience gained, and to learn from that experience. One of the key things that we did at the time was carry out some research into what the public feel about the use of CCTV.

Now, generally, the public were accepting of it. Even where they saw that crime might only being displaced -- that is, that it moves from the areas where CCTV is watching to areas where it isn't -- it was clear that the public saw some of the new things, such as having hidden microphones picking up conversations, the public were concerned about that. You won't be surprised to know that, though technology aimed at protecting individuals had quite a favorable reaction, speed cameras for catching motorists didn't; people were rather less keen on that. But what the public did do is, they did come up with some of their own rules of how they saw CCTV should be operated, and I'll touch upon these, briefly.

They felt very strongly that there should be clear signs. They feel that transparency showed much respect for people, for the public. And there are a couple of comments there from individuals. These are taken from the research. They show that people did have quite strong views about the use of CCTV. Moving on, the public were also quite keen that the images should be of sufficient quality, because they recognized that if they weren't, they weren't very good for crime prevention. And they were also particularly bothered that there should be appropriate security; they didn't want them tampered with, theft, or they didn't want there to be authorized –unauthorized disclosure.

There are some key messages here, I think: that they have a trust in CCTV, where they can understand the benefit. The major benefit in U.K. is seen as personal protection. But also what came out is that the public's trust can easily be eroded by poor operation. And I want to just stop here briefly, because I mentioned the Surveillance Society Conference that we had done, so I wanted to put CCTV into a wider context. We recently had a follow up conference into looking at particular aspects here. And what we did is, we did some research using focus groups, looking at how citizens felt, not just about CCTV, but about surveillance in general. The results of that were really quite interesting.

By and large, most people were relatively happy, initially, about the idea that both the private and public sector knew an awful lot of information about them. But, actually, the more that they thought about it, and particularly where there were specific examples drawn to them of how a surveillance technology might be used, they became much more -- much

more concerned. I think one of the interesting points -- and this is why I go back to the data-disks thing -- there is some evidence to believe that individual -- because of the degree of media attention, that, at the moment, individuals in U.K. are much more concerned about where their information is. Is it being looked after properly by private organizations and by the government? I think it's actually something that the U.K. PLC has had to recognize, and is in the process of seeking to take appropriate measures, because I think they do realize that if they lose public trust, there are real concerns there.

Finally, in the U.K., as I've already said, the U.K.'s surveillance technology, at the moment, is mainly regulated by U.K. data-protection and human-rights law. There are certainly some concerns in some quarters, particularly people who are interested in efficient use of CCTV for crime prevention, that the way that the technology has been introduced, often on a piecemeal basis, often without appropriate standards, really does mean that there's a need to look hard at whether there should be a body or some mechanism for ensuring the degree of interoperability, and ensuring a degree of technical standards, but also -- and this, actually, is probably something that's relatively resource-intensive -- where there's capacity for auditing and going and actually checking on systems to make sure that they're doing what they ought to be. This recent national CCTV strategy produced by the Home Office -- in ACPO and certainly the Home Office scientific branch -- has produced some detailed guidance on the actual technology that should be used. The point where we are now is that the revised code is about to be published shortly. Shortly means next month. That should be in January 2008. As I've already said, our research suggests that there is public support, but the public support depends on the public believing that there's appropriate control and there are appropriate rules which those who hold their information will be forced to abide by.

[Applause.]

MS. BALLARD: Thank you very much, Phil. We greatly appreciate the ICO's office for sending you across the ocean to join with us. We know you guys have been very busy, and we know we can learn a lot from the research and the expertise that you have in your office. So, thank you very much for that. Ken Anderson, with the Ontario Province Information Commissioner's Office.

MR. ANDERSON: Hello. International perspectives. You can imagine – you may have seen this, any of you that came in through an airport, or you've been to the newsstand lately -- the current edition of Popular Mechanics magazine has a really high-tech camera on the front, and it says, "Are You Being Watched?" And then there's a series of articles that are -- sort of, tell all, and they explain how the cameras work and what the philosophies are and so on. Don't know if you saw that, but, when I saw that, my heart sank, and I thought, 'oh, man, now I'm going to miss my trip to Washington, because you can just read this whole thing.'

[Laughter.]

MR. ANDERSON: And that dismayed me. However, turns out that we have some experiences, and, like Phil, we wanted to share these. So, we've come down here. Quite pleased to be here today. Our commissioner is Dr. Ann Cavoukian. She originally had accepted the invitation, was very keen to be here to meet with you; unfortunately, had a serious accident, had surgery, is recovering well, sends her best wishes. And so, I'm standing in for her. So, video surveillance cameras, a consultative, collaborative, cooperative approach.

What's the talk about? I'm going to talk briefly about our role, because sometimes for those people who are trying to implement the system, where you get the authority and how you get to do it can matter, so I'll do something brief on that, our work on video surveillance, or CCTV, some observations, and some best practices. And later on, you'll be able to go out to the table outside and pick up a copy of the best practices, put in a sort of a tips sheet, if you will.

So, role of the IPC. Now, in Canada we have a Federal government, so you've got a national government, and then you've got provincial governments, sort of like you have things coming out of Washington and you have things coming out of the States, and, of course, then municipalities and cities. We are an information privacy and commissioner working out of Toronto, Canada. That would be sort of like working out of New York, let's say. And so, we have to work together with our federal counterparts to make sure that we cover the waterfront. What we do is, through these three acts that you're seeing there, the Freedom of Information and Protection of Privacy Act not only includes privacy, but also deals with what I think you'd call down here FOIA, and is about information transparency. Then we have the Municipal Freedom of Information and Protection of Privacy Act. A bit misleading, because it's not just cities and towns, it includes police services, it includes schools, it includes an array of levels that aren't at the provincial level. And, finally, we have a thing called the Personal Health Information Protection Act, and that's like your HIPAA, I guess it is down here, and covers a range of things. And, of course, since we have socialized medicine, it has its own wrinkles for that.

What we don't cover is interesting, partly because, (a) we don't cover it, and (b) because we sometimes ignore that we don't cover it -- we do it anyway. So, what we don't cover is, we don't cover federal things like, well, antiterrorism, and we don't cover the RCMP, and we don't cover -- actually, in Ontario we don't cover private sector, so we don't cover individual businesses. But how our office has an interaction is that a lot of the people who are doing health work actually are businesses, like a pharmacy, like a lab, and so on. So, we design policies for them that actually can speak to the rest of the business organizations. We're the only legislation in Canada that has, actually, mandatory breach notification, in that last legislation, PHIPA, and so, because of that, we have a lot of people asking us about breach requirements, even though we don't legislate for the private sector. And, finally, we talk a lot about technology and privacy, and you'll hear some of those things today. So, I think that

even though our jurisdiction is bounded, we often are appearing outside and doing some other things.

So, the mandate of the IPC, we investigate privacy complaints, and we do some, I think, rather interesting things under that. We resolve appeals from refusals to provide access to information, and, in some cases, that access actually lies in what you would view as a privacy sphere. We educate the public about our access and privacy laws. We spend a lot of time on that. And we conduct research and access on privacy issues. I'm just going to skip through that and give you the results of some of these things.

Have to start with the approach of the commissioner, and you have a rather well-known academic and consultant, Malcom Sparrow, who has talked about the notion that you could take a good piece of regulatory legislation, and the way in which you implement it, you could really ruin the legislation. And so, the view of our commissioner is that she starts out with this consultation, collaboration, and cooperation, and the notion is that the value of privacy for us in our office is what Dr. Cavoukian describes as practical privacy, and that you have to weave it in with the other things that we need to do in our society. So, how do we make that work on the ground? Well, we, too, put out guidelines. I should tell you that we've had a lot of reference to our colleagues in the U.K., and, as much as you may have a lot of CCTV that goes on there and so on, in fact, their office does terrific work. If you haven't seen their publications, I can tell you that we get them out all the time. And one of the things we're doing later, I'll show you -- we're actually using some of your materials. So, we put out guidelines. They're very similar to what you heard from Phil.

A couple of things you'll want to know. Originally, this was a streetscape focus, and it focused on the common law, that notion that people have the right to be out in public spaces, and so on and so forth. But then we had to start thinking -- remember, with this municipal stuff -- what do you do about water plants, which are certainly in the public sector, but a very special space? What do you do about libraries or the legislature, police headquarters, and so on? So, we're not just moving our guidelines, we then sort of enhance them, but also the way in which they're applied, the context matters, just like the civil law and common law as it applied.

Toronto Police Services -- how does this come together? Toronto Police Services have done a number of things where they wanted to work in the public space with cameras. But, in some cases the cameras weren't permanent. What they did was, they put them up at the time of -- when we have, for instance, a car race there in the summer, or when we have a large event where there's, in the past, sometimes been some problems. You'll put up some portable cameras and take them down, so there's windows of time. But, finally they came to want to put up some cameras that were of an indeterminate time nature, but certainly for a long time, in an entertainment district, where you have 25, 27 dance clubs all together. There are thousands of people that pour out of these clubs at the end of the evening. The concern was

not for regular policing. They have mounted police. They have paddy wagons. They have people on foot beat. They deal with all the normal infractions. The problem was that, every now and then, unfortunately, there were shootings, everybody disperses, and they can't find witnesses. They wanted to do a program that would be specific to that, yet they still wanted to comply with the privacy issues. I guess we were in a fairly compliant society, so they actually come to our office and ask us about how would they apply these guidelines? And they brought their own ideas.

So, they went and did consultation in various parts of the city. They took us down to the proposed sites. They narrowed the sites down. They gave us a record of the assaults and shootings, and so on, in the area, and said, "look, all this stuff over here, we don't care about." It's just these three focused corners. It's not the traffic, and it's not the general partygoers, it's just to know when there's the specific events. And then what they did was, they used, like you said, Phil, very large signs to let everybody know this was there. Doesn't deter anybody. I think if you wander out of these clubs late at night and have a gun, you're probably still going to be there. But the point for them was the follow-up. Only certain technicians could access the cameras. They could only access that portion of time that was relevant to the event. The camera tapes are overwritten every few hours. Now, I have to remember, because we also have a bus project -- I think the bus project, they overwrite every 2 hours, and these ones, I think, overwrite every 6 hours. So, the camera keeps going, and, if there's been no event, they don't stop it, they don't record it, they just write right over top of it. It's not sent to a data bank, it's not going wireless, it's not in a digital archive; it just keeps moving on. So, it's very event-specific. So, we spent time with them, and they're still in the opening phase of the project, and then they're going to do an assessment after 6 months. So, that's one of the ways that we work with the different folks. We have many others. I'm not going to explain them, because I want to take your questions, if you have any.

I'll just mention that something that was kind of sensational for us was, there was a hospital in a city north of Toronto -- Sudbury -- and a baby was gone from the hospital, and, indeed, somebody had taken the baby. They were able to find the person that had taken the baby, and actually recover the baby securely. And the person that took the baby actually needed some assistance, themselves, as it turned out, and they were able to go off and deal with that person, as well. And so, there's been -- and I think, Phil, it's -- like the surveys that you've seen, there's been a high degree of acceptance of the idea, certainly in our society, that you could use the cameras and their aftereffect in ways that were important for the society, but how could you deal with some of the privacy issues in between?

Which brings us to Privacy International. Some of you may know them. Certainly, you'll know them, out of England. We received a complaint from Privacy International -- it was filed under our legislation about our Toronto Transit Commission. I think we have something like the third-largest transit commission in North America, in terms of dollars and

track and so on, partly because we're spread out, like Los Angeles, and just have a lot of miles of this stuff. So, we've taken in the complaint. We are currently processing it. I'm not going to say too much about it. Obviously, we're going to use our guidelines. We're going to look to some of the work that we've done, that academics have done, you'll hear later, in Ottawa and down in Queens University also, in Ontario. But what I can tell you is this, is that one of the aspects that -- and you can see the complaint -- you can see on the site, one of the things that our commissioner has focused on is privacy- enhancing technology. The notion that, just because there is a camera, just because there are many other things -- computer data banks and so on -- doesn't mean that we have to lose the benefit of these, and it doesn't mean that we have to forego our privacy. So, the idea is that you try and take the technology and work with it to achieve both, or multiple, ends.

In this case, one of the things that we're looking at, and will spend some time reflecting in this order, is the notion of face-blurring. You've probably seen some of this, because there are a couple of different versions of it out there now, and there's a problem with all the versions that have been done to date; like, most technology, 3 years is a long time. In 3 years, this stuff's come a long way. But, what's the problem? Most of it is this type -- you know, you used to see in the National Enquirer, where you see something like this or like this and some -- and you can't undo this blank space once it's recorded. There are some people at the University of Toronto that are doing some work, where you take the picture, and you still can blur the face or faces, and you can do it in a way that's encrypted. So, now we're after them about biometric encryption and all of that. But you can unencrypt it or decrypt it when necessary. And then, how do you do that, and what's the protocol, and do you have special keys, and so on? Are there opportunities to apply that in this kind of a system? The other thing that we'll do is also spend some time on, as Phil said, some of the things beyond just the collection. What about proper maintenance? What about proper use? Making sure people are trained. Where does that information go? How does it get disposed of? Why do you have to keep it forever if nothing happens? Indeed, why do you have to keep it even a very short time if nothing's happened? So, we're going to spend some extra time on that. Later, in questions, if you want to ask anything about that, I'll tell you a little bit about how labor relations has factored into that case.

Best practices for using CCTV in public places, we have best practices which are much like the kinds of things you've talked about, Phil. As I say, we're going to hand out copies of this so you can look at it for yourself. Wanted to highlight a couple of things. One was that, when you're developing these accountability frameworks and so on, that some of the default is 'do you really need to do this in the first place?' Because you want to minimize data. If you don't need to do it, if you don't need to collect, don't do it. If you only need certain information, don't collect everything else. If you do need to collect it, keep it for a very short time, and so on. So, data minimization is a frame that goes throughout this.

Also, doing things like privacy audits, security assessments, threat-risk analysis, doing later audits to go back and see how this is working out. The Toronto Police and the transit people have actually built these kind of things into the projects that they're doing so that they come back to them. And, I think, if you keep looping back, there's a chance to say, "this isn't a one-chance deal." As you know with encryption, you started out doing stuff with DES, and then, triple DES, and you go to elliptical and all that stuff, you don't just sit there and say, "well, now that I've got it encrypted, I'm not going to pay any attention to how the world's going on." So, we're encouraging people to keep coming back and revisiting that. And so, here's how to contact us. And wanted to mention two things. One is, there is some active work, sort of, piloting these ideas, from the University of Toronto, to test out how they do the filming and the blurring. So, if anybody wanted to talk to our office about that, we can put you in connection with the two professors that are doing it. They're also doing some biometric encryption work with us.

And the second thing on the feedback is simply, in that Popular Mechanics article you'll see that one of the little pieces is something on the people who are being filmed filming back. And, of course, the original idea was going around with cameras that were very obvious. Now, of course, people are using cell phones and BlackBerrys and snapping photos. There's also a professor in Toronto who has done a lot of work on what he calls "sueveillance", as opposed to "surveillance", and this whole notion of filming back. And you might just want to see the popular view of that in the magazine. So, thank you so very much for having us here.

[Applause.]

MS. SAADAT: Thanks very much for that presentation, Ken. Now I think we want to turn to Professor Norris and Professor Deisman to start the discussion going. And, again, we're going to be breaking a little early for questions. I think Professor Deisman has a short presentation he wants to show.

MR. DEISMAN: .I'd like to begin by thanking the organizers for inviting me here today. This is actually my first visit to Washington, D.C. And I came to Washington, D.C., as a single eligible male, and I'm happy to say that I'll be leaving as an engaged person.

[Laughter.]

MR. DEISMAN: My fiance and I were engaged, the night before last night. And –

[Applause.]

MR. DEISMAN: -- I've got to say, what a magical city to do it in, and what a fantastic place, that people have been so wonderful.

[Laughter.]

MR. DEISMAN: I don't know if it was caught on CCTV, but I'll be looking for the footage, because, geez –

[Laughter.]

MR. DEISMAN: -- what a thing to look back on, 20 years from now. The talk I want to give today is based on a series of researches that the National Security Working Group, located at the University of Ottawa, has been doing, trying to arrive at a comparative understanding of what's happening in advanced capitalist Western democracies in response to the specter and threat of terrorism, and particularly, how policy instruments are being mobilized, policy choices being made, and legislation being formulated, in response to the perception of the threat. I should say that the researches that we're involved in are still at an inchoate stage of development, they're still nascent; and, for that reason, I won't be presenting a full-blown argument either for or against or with any definitive sort of take on CCTV or the best practices associated with them. But what I would like to do instead is have an open and, kind of, exploratory investigation with you of some of the issues associated with CCTV and the, sort of, broader historical background context that, really, I think we should all acknowledge, kind of, puts us here today, and has us here today, thinking together about whether it's a good idea to go forward with CCTV, and in what ways we ought to go forward together.

I wonder if I might begin, though, by asking you to indulge me in an exercise I use with my students when I teach this stuff in my advanced terrorism risk and national security course. I wonder if I could ask you to take out a blank piece of paper for me. Yes, this is the audience participation part of the seminar today. Take out a blank piece of paper, and, if you would, just indulge me by writing three or four -- writing down three or four characteristics or attributes by which we might identify a terrorist in our midst. Three or four attributes or characteristics by which we might be able to identify a terrorist in our midst. Just jot those down quickly

[Pause.]

MR. DEISMAN: Okay, I can't afford to give you too much time with this, or I'm going to get the cane and yanked off the stage. So, how many people had four attributes?

[A show of hands.]

MR. DEISMAN: Three?

[A show of hands.]

MR. DEISMAN: Two?

[A show of hands.]

MR. DEISMAN: One?

[A show of hands.]

MR. DEISMAN: None? How many people had none?

[A show of hands.]

MR. DEISMAN: Alright. Okay. So, I'll just ask you to hold onto that paper; I'm going to come back to it and use it in a bit, here. I'm going to talk about CCTV today, and I'm going to be employing what's called an imminent critique or -- there are two kinds of traditions in criminology, in terms of the analysis of policy. One is called the transcendental critique, which questions both the aims of the policy and the means used to achieve that policy; and the second is called an imminent critique, which really examines the means which are proposed to achieve particular ends. And I think the objective of fighting terrorism, of fighting crime, is relatively unproblematic and doesn't need to be challenged, although we could look at how the threat of terrorism has been constructed.

The main thing that I really want to do today, and the tradition I'll be leaning on and leaning towards, is called the imminent critique, which really looks at the means. The means I think we're looking at today are CCTV. And I want to, sort of, qualify that idea about CCTV in a second. But, really, I think the key question is this question, whether CCTV will work, or does it work, I think, in combating terrorism and combating crime and making communities safer, more generally? I want to, sort of, unpack my own biases right at the beginning. I've been doing work on CCTV, like Clive, for quite a long time, and I have to say that I'm quite dubious about CCTV and its effectiveness, for four different types of reasons. The first, and probably the most important, is that the empirical record with respect to the successes of CCTV is pretty mixed. And there is definitely no definitive evidence to show that it's effective in any situation in relation to all kinds of crime. In fact, I would say that there is currently a great deal of dissensus amongst the academic and scholarly community about its effects. There is, however, widespread agreement that it can have serious effects on our civil liberties and on our core values, like privacy.

The second one is that I worry that CCTV may do more harm than good; and, third, that it may be a disproportional response to a particular kind of construction of a problem. And, finally, and perhaps most importantly, and perhaps in a sentiment that the audience may be able to identify with, I worry that it may promote a misleading idea about how security is possible in the first place. Okay. So, my aim today isn't going to be to convince you, or sell you, on anything here, but it's more in the spirit of a kind of case study or inquiry into a kind of particular way of thinking about prevention, and the limits of that kind of thinking.

I'm a criminologist by training, and we spend a lot of time thinking about crime prevention. And we distinguished between different sort of approaches to crime prevention. And there's an approach called primary crime prevention, and it looks at, kind of, what we might call the root causes of crime in the first place. It looks at poverty, education, those kinds of things. And there's another approach, called secondary prevention, which really is about trying to stop an illegal, immoral, unlawful act before it actually happens, but it's almost -- very close to just-in-time kind of prevention, and that's really what we're talking about in the case of

CCTV. So, I'm going to present you with a sort of understanding of why this issue of CCTV should arise in the first place today, and some of the historical, sort of, factors that need to be thought about, particularly in relation to this issue of terrorism.

I have four objectives, which actually have been now pared down to three, in terms of time, to describe what's happening in four countries. I'm going to talk about the United States, the U.K., Australia, and Canada. And to talk about one commonality in the approach that seems to be adopted towards terrorism, and then to describe some conceptual and theoretical resources that will help us think about this issue of terrorism; and the use of CCTV to fight it, and then, finally, to look at some of the impact and implications for civil society of this particular approach. So, there are two, I think, important conceptual preliminaries I want to offer, or make, before we go on. And I think it's really important to surface both of these, because, thus far, the discussion hasn't actually entered into both of these issues to anybody's satisfaction.

The first one is that I think one of the main reasons why we're here is, we're talking, now, not simply about the private employment of CCTV, which has been going on for a long time, but we're talking about governments adopting the use of these surveillance technologies. And I think, then, we need to acknowledge that what we're really talking about here is the use of these technologies in public spaces. And when we start to talk about public spaces, it's very important that we acknowledge that the character and nature of public spaces is in a process of profound transformation right now, that the nature of public space has been in a process of profound transformation for about the last 20 years, but many scholars say that it's been diminishing quite significantly, but most scholars agree that it is characteristic of the nature of public space today that it is cathected over by a variety of different, sort of, conflicting interests and characterized by a complex, sort of, intersection and interweaving of both private security and public police and a variety of other different regulatory agents who are all involved in this very complex latticework of surveillance, monitoring, policing, issuing citations, all of those kinds of things, so that public space has become quite a complex space. And the other, I think, important thing to note is not just that it's become complex, but there's been a significant blurring of the boundaries between public space or private space. One of the ways that I demonstrate this easily is, if you imagine the path upon which you traveled when you departed, this morning, until you arrived here at the hotel, and tried to define which of those spaces you occupied were actually public or private, I think you would have a real difficult time trying to decide. Are you here now in this hotel in a public space or a private space? Well, the answer is, actually, you're in a private space -- involved in a public activity, no less, but a private space. There's very difficult judgment calls associated with that all along.

Now, the implication is -- and it's a very important implication -- the implication is that there are no real, pure public or private spaces anymore, that the relationships are much more

complex. For our purposes, it means that we should think, instead of locational spaces, that we should think in terms of flows, about people flows, and, particularly important for the purposes of CCTV, we should think about data flows, because what CCTV does is, it creates a data double of you and your activities at a particular location, and creates an archive of it somewhere. Okay? That's the privacy issue. That's one of the privacy issues associated with it.

So, that's one of the conceptual preliminaries. The other one that I want to note is in relation to the first panel, and I think it was a theme that was emerging during the first panel, but I don't think was quite fully surfaced, but needs to be surfaced. The title of this talk, or this conference, is CCTV: Best Practices. But, as emerged in the first panel, we're not really just talking about cameras anymore, we're talking about a full range of sensory devices. We're talking about, yes, visual- capturing devices, but we're also talking about audio- capturing devices. And now we're talking about in places like New York, we're talking about olfactory systems that have the capacity to smell the air. Okay? And now we're also talking about systems which also can link up with radio frequency identification devices. So, we're talking about a much more complex – and the term that the theorists use this about a much more complex "assemblage" or "mélange" of a whole bunch of different monitoring technologies all meeting together.

So, CCTV is the public face, but I'm stressing this because, as somebody who's studied the history of technology for a long time, I know that technologies always ought to be understood to be on a certain trajectory of development. Okay? I think what we need to understand, in relation to CCTV, is that the trajectory of development is one of converging with other technologies. I say this, because the privacy issues associated with this are not going to go away. All of the forecasting says that they're only going to get more serious -- right? -- as the technologies become more and more precise. So, I think it's important to, instead of, sort of, reifying and having this, kind of, notion that CCTV is a fixed thing to notice right away, that it's a very slippery concept that we're trying to deal with. We're actually dealing with a very complex cluster of technologies that are morphing all the time into different kinds of relations.

If my demonstration, or my discussion, about the edge technologies, the monitoring technologies, wasn't enough in and of itself, we also know that CCTV -- that the advanced cameras that they're using now are Internet-protocol-equipped cameras, which means that they can also interact, intersect, and interrelate with the Internet. And this is very important, because about 3 months ago or 4 months ago, somebody made a Webpage describing for people, just general laypeople, how they could go onto the Internet and actually hijack publicly available CCTV cameras and take control over the footage that they were showing. Okay? So, that kind of interaction and intersection is very, very important for our purposes. So, those are my two conceptual preliminaries.

[Laughter.]

MR. DEISMAN: What I do want to talk about is the commonalities that seem to be characteristic of the four countries that I'm talking about. The four countries are characterized by one dominant assumption that informs fundamentally how the toolbox is seen.

You may remember, from this first panel this morning, that the discussion was about the toolbox. Okay? The toolbox is seen in a different way as a result of this one dominant assumption. And the dominant assumption is that the events of 9/11, and the events of 7/7 in Britain, produced what we would call a state of exigency or a state of emergency, or an extraordinary state. Okay? An extraordinary state. And it's characterized by these kinds of assumptions, actually. Okay, that the events of 9/11, or, conversely, the events of 7/7, what they revealed was not a threat to some portion of society, but a threat to all of society, to the very existence of society itself, and a threat to society as a whole, if you will. And this has an important consequence for how the toolbox is seen, and seen differently. What I say is, it radically reconfigured the field of intervention. It made choices contemplatable that otherwise would not have been contemplatable. I think the best and most compelling example I can give for this is that now, in the United States, on the table is this question of whether widespread CCTV surveillance should be used; whereas, 10 or 15 years ago, this kind of proposition, many people would have thought was ludicrous and unnecessary. There's all kinds of other examples that I'll give.

But I think the best way of, sort of, understanding how this idea about the state of exception works is to think about the pronouncement made by Dick Cheney. Dick Cheney said that, after 9/11, we were living in a condition he called the new normal. The new normal connotes this idea that the baseline has shifted, and it's shifted fundamentally. As a consequence, extraordinary measures are necessary; not quite anything goes, but it gets to be pretty close to it. So, I'm just going to talk about four trends, quickly, in relation to that. Okay. I'm going to have 1 minute by the time it gets to the slide I want. Alright. So, back one, and then we'll go.

Characterized by four different trends in these societies. This is Canada, the United States, the U.K., and Australia. The four trends are tipped scales -- and I think this was raised earlier, and surfaced earlier -- but this idea that there needs to be a balance between security and police powers, on the one hand, and civil rights and civil liberties, on the other hand, has morphasized into something different. I think the way that it's changed is to say that many people today believe that it's necessary to exchange some civil liberties or freedoms in exchange for more police powers and more safety or security thereby. That's quite a novel and important equation in the context of democratic societies.

The second one is that a particular idea of security has become what I would call hegemonic, and it's the idea of security built around technology or a kind of technophilia that says we

can have more security if we have more technology. And there are serious consequences associated with that way of thinking.

The third one is a general attempt to mobilize and enroll the public in a variety of different ways, particularly in relation to watching campaigns or surveillance campaigns. We've seen this in England in a campaign called You Are That Someone. In the United States, it's called the Rewards for Justice Program. In Australia, they have a public campaign, and they have that in Canada, too.

And, finally, this idea of Panopticism Plus, which I believe is at the heart of the CCTV initiative. It's this idea of a comprehensive omniveillant, if you will, watching program that sees, that smells, that hears, and that is integrated with these other seismic devices, with radio frequency devices, with all of these kinds of things. So, I'll close it at that and look forward to your questions. Thank you.

[Applause.]

MR. NORRIS: Well, thank you very much for inviting me. I do not have a PowerPoint presentation, but –

VOICE: Yay.

[Laughter.]

MR. NORRIS: Ah, thank you. I did, last time I came to see the Department of Homeland Security Privacy Committee, produced them a paper, which I'm sure can be remade available, because it's on their Website. That paper addressed many of the issues that we've been circulating today.

So, I don't want to talk for very long, but I want to raise what I think are four key points that come from my understanding and analysis, over the last decade, of the growth of CCTV in Britain, and then looking at the European growth, and not so much growth, and then thinking about what's going on in America now.

In Britain, I have guesstimated -- I stress the word "guesstimate" -- that there are 4.2 million CCTV cameras. Nobody actually knows how many there are. The information commissioner's officer doesn't. No one else can. I've talked at industry conferences, and people have said, "mmm, that might be about right, based on the size of the market and the length of time." I estimate that over a decade, between 1995 and 2005, about 5 billion pounds was invested in the industry, and at least half a billion of that was public money. A lot of it comes from private money. A lot of it is mixed money, not so easy to tie down.

So, one of the things I'm interested in about this technology is, if we're spending that much money, what's its purpose? What's it for? I think one of the things that interested me very much about this morning's conversation is that it reminded me of the conversations that were being had in England 10 years ago about when CCTV first really hit the scene, but in a

digital age. We were all analog then. What has emerged since then about that is, it's almost impossible to answer the question, What is CCTV for? Because if you say the purpose is crime control, and it doesn't work, or a study shows that it hasn't worked, someone says, "Ah, but, no, really what it's about is reassuring the public." If you say it doesn't work in that, they say, "oh, but it's a great management tool for deploying police resources", and so on. There is always another reason for having CCTV.

Now, this creates a really interesting problem, because if you want to put in and spend public money, it seems to me you should be able to determine what it is it's going to achieve, and actually, you should evaluate it before you spend the public money on it, and then determine whether it's a good use of resources. In Britain, public money was not spent on evaluating it when we first launched CCTV. As far as I can tell, the story is rather similar in the USA. There have been very few evaluations. But, more than that, in Britain, when the evaluations have come back, they have had very mixed messages. But, actually, the most recent and most authoritative evaluation, sponsored by the Home Office, says that its effects are highly limited, if any, in both the reduction of fear of crime and the reduction of crime.

Given that was the primary reason that CCTV was sold in Britain -- that was the primary reason – one might think, therefore, that maybe some schemes would be stopped. But, no, they haven't, because other reasons have always been given. So, I think we have to ask ourselves, you know, what is it for? How are we going to judge it? What do we do when we get the results of that judgment? Otherwise, I think, as people who are responsible for informing the debate about public money, we're failing. We often, also -- and I've seen a number of documents related to this particular talk -- we talked its antiterrorist role. But we do have to remember, it didn't stop the London bombings, it helped, afterwards, in tracing a network. But if we see it as a preventative tool, it wasn't very successful. Maybe that's what we have to think about, whether there are other things we need in place.

I'm going to make two other points, because I don't want to talk too long, because I think we need to debate these issues. The third point I really want to look at is, we do have to worry about the cameras and the visual image of people, and how that is regulated and controlled. But, actually, for me, one of the most pressing issues -- and I think it came out very -- very, very well in this morning's presentation by the technologists -- is that, actually, it's the computer, not the camera; it is the system the cameras are embedded in, that we have to look at. Actually, it's the database.

Now, I was really relieved that facial recognition was not really touched on very much this morning, because it's been a sort of holy grail that hasn't really delivered. But let us look at the British case, because facial recognition was put in, in London borough, and hyped all over the world as being the solution to crime control, but seen to fail. But those same cameras, the cameras that were put in local High Streets, but also have now been linked to those on garage forecourts and so forth, are very good at identifying another identifier, and

that is a license plate. A license plate is much easier to read. If you can read a license plate, you can identify it to a record of the vehicle owner. If you can do a record to the vehicle owner, you can then link to the police national computer in Britain. If you can link to the police national computer, you're then talking about access to millions of records, as well as a whole range of other databases, such as insurance databases. Okay.

The U.K. Government's view of this is that this is a really very useful tool, and they have a document called Denying Criminals the Use of the Road. The vision of that is to store 50 million records of vehicle transactions across the country every day, and keep them for 2 years. This means we can have a total pattern, or partial pattern, of movements of people, linked into various databases through this. This is a consequence of the technological infrastructure that has been created. If you asked me, in 1996, when I started researching this, would that happen in 10 years, I would have said no. But it has happened now. And this is what we have to really think about. And I concur, absolutely, with you, it's, where is the trajectory?

My final point is about data protection. Oh, I have to do this -- well, not appearing to undermine my colleague, but from the Information Commissioner's Office, who I'm very fond of, but I don't think the U.K. is the place to look if you want to know how to regulate CCTV. I think there are other European examples which have different models. I'm saying this for a number of reasons. Partly, it is about the nature of the particular regulatory framework. The aim of regulation in Britain is not to restrict the use of CCTV, in the sense that if you say its purpose is for the prevention of crime or for the enhancement of public safety, it is then a legal system, in that sense. You don't need any special justification. In other jurisdictions, that would be quizzed or inspected or argued about; in Britain, it's not. So, actually, the basis of the regulation in Britain is really to license something, it is not to restrict it, and that is a very important point.

The second issue in relation to this is the actual data-protection principles contained within the Data Protection Act, these seem to be perfectly reasonable and right. I don't have a problem with that. But the resources of the regulators of the Information Commissioner's Office make it almost impossible for them to actually ensure compliance. What they can do is, they can chivvy along. I think, particularly with public authorities, they have been quite successful in doing that. I have, you know, great respect for that. But there are hundreds and thousands of schemes; it's just not possible to do. If you take one issue of that, the issue of signage -- when we looked at signage in an area of London, we found that, in our judgment, 78 percent of systems did not comply with the Act. So, passing laws is one thing, but actually making a difference is another.

The final point I would make is that CCTV footage is gained without people's consent. And, indeed, when my family's car number plate is recorded and entered into a database, it is done without my consent. And, generally, that seems to me to require special and rather more

heavy-handed regulatory intervention than that information that we give freely with our consent. And I will stop there.

[Applause.]

MS. BALLARD: Gentlemen, I want to invite you to engage in a discussion for about 10 minutes, and then we'll have questioners come to the mikes from the audience. Any question that either of you would like to pose to –

MR. NORRIS: Would you like to respond, Phil?

[Laughter.]

MR. JONES: Yes, I'm going to try and respond gracefully.

[Laughter.]

MR. JONES: I think that two points Clive picked up on that I think are really quite important. One of them is a resource issue. Clearly, if you've got as many cameras in U.K. as Clive's best guesstimate is, of 4.2 million -- and, interestingly, I even saw that over breakfast. His figure was there in USA Today. It was in an article to do with Tescos Car Parking. But your estimate got in there. So that if we are talking about that many cameras, clearly there is a massive resource issue in having an organization that is set up to properly police, properly check, properly audit. That was part of the reason for pointing out, at the outset, that our responsibilities, as a fairly small office, are to deal with a whole range of applications of data protection. That's the first point I would make.

The second point -- I think this is quite an interesting one --, I think -- one was historical, that, actually, when we came to start regulating CCTV, by that stage the horse hadn't only bolted, several racing stables had run all over the place, and we really were coming in to a situation which isn't where, in an ideal world, you would like to start. But, actually, I think there's something probably more fundamental than that. It's an interesting point, that, when you're applying data-protection legislation, different European jurisdictions apply it in different ways. Because it seems to me that there are -- to a very real extent, we are quite heavily conditioned by what the public seems to expect -- what the public, on the available evidence, seems to expect. Interestingly, there are jurisdictions where the public would see CCTV cameras as an anathema, but they would be quite happy with ID cards, which not everybody in U.K. is convinced about. It's one of the interesting things, is that you inevitably are constrained, in my view, to some extent, by what the public will accept.

This takes me to the final point. Clearly, one of the difficulties that we have -- and we have it in lots of areas where we give advice, so there are even things that I don't really care about at all, like advice on marketing -- sometimes people come to me for advice on marketing strategies, which seem to me to be mad. But I'm not a marketing expert, and I can only tell them whether I think it seems to be broadly fair. But, Clive's quite right, whether something

is worthwhile is whether it actually achieves what it's intended to achieve. I think the interesting point about his comments about the Home Office study was, this is the same Home Office who is very keen to set up a board to drive forward greater integration of CCTV cameras. It's quite an interesting position there. And I hope that wasn't too unduly defensive, Clive.

MR. NORRIS: No.

MS. BALLARD: Any other comment?

MR. DEISMAN: -- I guess my question could be for either of the regulators, and certainly for the audience, more generally. But, I think one of the themes that emerged this morning, and particularly during this panel, is this idea that technologies are on paths of development, on trajectories of development. In the case of CCTV, it's not really just CCTV we're talking about; we're talking about a whole assemblage of surveillance mechanisms -- smell, et cetera, et cetera. I'm wondering whether either of the regulators would care to comment on, sort of, how that interface with industry actually looks, so that we're not always in a position of having our laws and regulations running 4 or 5 or 10 years behind the technologies.

MR. ANDERSON: Well, since Ottawa is in Ontario, I'm happy to respond to that one.

[Laughter.]

MR. ANDERSON: I think we do it in two or three ways. First of all, by and large, we -- and I don't disagree with the things that either of you gentlemen have said; there's a particular contexting, and I'll just stay, Wade, with the ones that you've posed -- in terms of the assemblage and so on, I think part of the notion is that you have to get the intention --go at the intention, in the first place. So, as you said, for instance, Clive, What's it for, and are you getting the value that you wanted to spend for, and so on? So, a thing that could have happened when the -- when the Toronto Police -- so, I'm trying to bring this down to a very specific space -- when the Toronto Police wanted to go forward and do some work in response to a particular problem they were having, it wasn't a problem where they thought that cameras -- and, in fact, cameras, alone, in particular -- was going to drive away this problem about the shootings and so on. You have many other elements that you have to deal with. You've got to be figuring out who's there with guns, and why I've got guns in the street in the first place, and whether or not you have metal detectors in the clubs, and many, many other things. So, you do the consultation, and you drive it down to saying -- this isn't in a wall of cameras -- it's not 1,000 or 10,000 or whatever -- this is three cameras specifically placed. I agree, especially, with your notion that these things are set in systems, and so are RFIDs, and so are all of these other things -- so, is there, or is there not, a database? And how do you achieve that database? And where's your threat/risk analysis? And how soon can you properly and securely dump a database, if you had it, and so on? So, in this case, they're not automatically building a database, and they don't send it by, you know, wireless, and so on.

So, I think the more things that you can do to address -- not attack, but address -- each of those important issues, helps put it in context, because, you know, these things are popping out all over, and there's many aspects to it. We don't think that the work we do on privacy-enhancing technology is a single type of response, and I don't think, otherwise, that the technology is certainly seen by the police as being a one-off response.

And I might just throw in one other thing on these privacy impact assessments and doing consultations. This has got a lot of feedback, doesn't it? I've got to sit way over here so I don't -- is two different notions of consultation. One is, we did a consultation at a very fairly small city on Lake Ontario, called St. Catharines. I don't know if any of you know where that is, but it doesn't matter. The point is, the business improvement area -- it's not always just public sector, of which I'm part and many of you may be -- but the business improvement area decided that they thought they needed a sort of a safer view on the ground. Now, they had hardly any crime, as such if you really looked at the stats. But they wanted the notion that the streets were safer, and they're creating this downtown focus. They came together with the police services, and the police services actually came to our office, again, and they engaged the general public, the municipality, the business improvement area, which was made up of merchants, primarily, and the police services. The net result was fascinating. In the end, the public and merchants said, "what we really want are police on the ground." And they said, "in the summertime, let's go with police on bicycles", because that also had a certain friendliness to it and created a certain ambience. In the wintertime, people will get out there and walk the traditional beat through the snow, and so on. That's what they did, and they never did put up the cameras, having gotten together, ostensibly, on a CCTV consultation meeting. So, I think going through processes can have payoffs.

MR. NORRIS: Can I respond to that? Because one of the things someone said this morning, was about having an automatic gunshot detector. I immediately turned to Phil and said, "Wait. If a gun goes off, surely a member of the public should ring you."

[Laughter.]

MR. NORRIS: Do we need an automatic detector? I make this in absolutely response to this point here, is that we can have two different models of policing. We can have a model of policing where police live outside the city on their high ground and come down when there's a problem from their privileged space and impose order, and do it through all sorts of technologies, or we can have a model of policing which is, police are part of a community, are responsive to that community, are integrated with it. When they are integrated with it, what they get is information, they get trust and respect. We're in danger of going for the technological solutions of actually creating a police force that comes down from the mountains to impose order, rather than one that i actually part of our communities. And that is what we have to facilitate.

MS. BALLARD: If we have members of the audience that would like to pose questions.

MR. YANG: Good morning. My name is Press Yang, from FEMA IT. I think we can all agree that there's more violent crime in the United States than there is in the U.K., Canada, Europe. There's also the perception that the citizens of the U.K. are more accepting of video surveillance. So, clearly it's just not a case of violent crime. That being said, to what extent do you think – clearly, you, in the U.K., have had to live under the specter of terrorism much longer than we have here in the United States -- so, to what extent do you think that plays into the acceptance of your citizens to video surveillance?

Additionally, that being said, there is also a limitation to what your citizens are willing to accept, as evidenced when it became public that the airlines had disclosed passenger information to the U.S. Government. Also, there's a backlash from Europeans to our efforts to fingerprint foreign visitors to this country. So, there clearly is a limitation of what your citizens are willing to accept. And, having said that, another comment I'd like to make, to Mr. Norris, is you had said that video surveillance didn't prevent the London bombings, but it could probably be argued that they did lead to additional arrests that may have prevented additional bombings. So, that could be argued. And I'm just playing the devil's advocate there.

MR. NORRIS: Yes, CCTV does sometimes stop crime. If you look at the evidence, though, and general rates of crime, it doesn't seem to have had a great impact. If you look at the specifics, you know, it didn't stop a number of things happening. Of course if you have that many cameras, it will find evidence.

But one of the problems is that people seem to think that this is a magical solution. It just works. It doesn't. If you took one of the really problem -- oh, well, one of the terrible terrorist incidents in Britain was the Brixton bomber, who put bombs across London. It took a team of 60 detectives over 2 weeks to go through the video footage to actually locate that person. That's a huge amount of resource. It wasn't just that the image was suddenly there, because there were all these cameras about. Because of things like multiplexing and the fact that they were pan-tilt-zoom cameras, it doesn't work like that. So, it's not an instant solution. Indeed, actually, it's clear, in the Brixton bomber base, that other methods, other forensic methods, would have probably identified him at about the same time that they got the video footage.

MS. MULLIGAN: Dierdre Mulligan, UC-Berkeley. Clive, I was actually going to ask you to talk about that, because the idea that the video camera helped "catch them" is this interesting -- the technology coming down from on high, and saying, "oh, here's the person you wanted." And the behind-the-scenes -- this was a 60-person, multiple- man-hour -- it just shows the light on what resources were required to make use of the technology. But I wanted to ask, in thinking about framing the conversation, -- there's some pushback from Clive and, I think, from Wade, saying, "well, privacy impact assessment, data protection, it doesn't seem to be getting us closer to less surveillance or more thoughtful deployment of

cameras", but I haven't heard either of you present another model. Community policing, yes. But what's the decisionmaking process that you think gets us closer to, perhaps, less surveillance or more realistic uses of technology in the context of policing that doesn't have us on the mountaintop, has us more on the ground?

MR. NORRIS: I think, actually, perhaps listening to what the public have to say. As in Canada, if you ask the public what they want, what they want is human presence. It's not that they want less surveillance, what they want is reassurance, reassurance from people who are authorities in particular situations, people they can see and talk to. The idea that security is gained by a camera -- well, whose security is gained? In a sense, it's somebody else's security. Because the security that's gained, if you're on a London station at 8 o'clock at night in the dark, and there are no guards on that platform, no personnel on it, and there's a help point coupled to a camera, that, if you push, will ring an alarm 12 miles away and will deploy someone, well, by the time you've been robbed and are laying there in the gutter, they may manage to get you an ambulance. I'm not sure that's security. And so, that would be my argument.

VOICE: But wouldn't society be more secure if you captured the perpetrator that crimed him? Wouldn't that make the society, as a whole -- maybe you, the person lying on the ground –

MR. NORRIS: I think it would be more secure if there was someone there who had deterred the person from doing it in the first place.

MS. BALLARD: Next question?

MS. OZER: Nicole Ozer, from the ACLU of Northern California. Clive, your comments, that some of these discussions are, sort of, reminiscent of discussions you heard 10 years ago in Britain about CCTV -- and I had just seen, in September, that the liberal democrats of the Assembly had put out a statement, saying that, you know, much of the CCTV, in their view, had been a knee-jerk reaction, and calling for, sort of, a broader discussion of the role of CCTV and what it should be in Britain. So, Phil had discussed a little bit about creating new standards. I just wondered what the status is of actually having a broader discussion about the role of CCTV and whether it should continue or expand, or whatever, in Britain. Both to Phil and to Clive.

MR. JONES: Two things. I don't mean to be rude about the liberal democrats, but –

[Laughter.]

MR. JONES: -- if you know our politics, they can say quite a lot of things, and some would argue it doesn't matter very much, because they're the third party, and they're likely to be the third party for the same time.

Having said that, I think that we certainly -- in our position, at the Information Commissioner's Office, it's quite impossible for us to commission all sorts of thoroughgoing research into all sorts of different -- the effectiveness of all sorts of different technologies. Now, we would try to encourage these, as far as we can. So, anything that contributed to a more evidence-based debate about whether CCTV and other technologies should be -- continue to be rolled out in the way that they're being rolled out, that's something that we would hugely support. As I say, the problem is in terms of resources. We might think it smells wrong, or we're not convinced by the arguments, but it's pretty hard for us to produce the conclusive, you know, killer evidence that puts the position clearer.

MR. NORRIS: I would welcome a debate in Britain. I think the public are broadly happy with what they see. I think one of the issues is, I don't think they understand how these technologies are converging. This is the point that was made here. I think Phil's point about when they started talking to people about how the world was moving, people became much, much less supportive. So, in one sense, it's partly about education. And that's one of the reasons why the debate that's going on in Britain now, I think, is important. There is a big debate going on about the nature of the surveillance society. Some of these things are now starting to be discussed much, much more openly, and much more intelligently.

MS. BALLARD: We'd like to finish up the questioners that are in line so we don't delve into everybody's lunch hour. So, if we can keep it concise, please.

MR. ERICKSON: I'm Stan Erickson, National Institute of Justice. A question. First of all, I was a little surprised to hear such negative comments about the effectiveness of CCTV, and so on, in the evaluations that had gone on. But I do know, from our own experience at NIJ, that doing evaluations is very difficult. There's a lot of complicating factors that come in. Crime is very local, and it's temporally fluctuated by a lot of environmental factors, and so on. I'm wondering if the studies that you're privy to have covered some more, possibly, easier-to-measure things, like number of cases closed with the addition of CCTV, versus without, and so on, that might provide a easier measure.

MR. NORRIS: I agree with you, it is very, very difficult to look at effectiveness. That's one of the problems, is that a lot of very poor science has been done in the name. When you look at the good science, the good science tends to suggest it has much, much less effect, if any, than the bad science. When you look at the specific about case closed, I mean, in a sense, if you have a system, and it spots someone kicking someone's head in, and a police officer is deployed, case closed, almost. That doesn't tell you so much about the effectiveness of CCTV, in response, because it may have been closed anyway. Just that bit doesn't help. But the answer is, there isn't a huge amount of evidence to suggest that it increases the clear-up rate, either, which is, I think, the question you're asking.

MR. ANDERSON: Could I just make an add-on to that, in terms of, sort of, acceptance rates? We don't have a lot of very special, magical metrics, but two things that have been,

kind of, interesting. Out in Edmonton, in Albert, in Canada, the police force did something similar to what the Toronto Police are now doing, maybe 4 years later, which is to put up cameras in a particular entertainment district, and especially if the hockey team was especially successful. You had people taking to the streets, and a bit of mayhem, and so on. Interestingly enough, they did their own internal review. Unfortunately, we don't know what the review is, because it was closed into that police community. But they came to their own decision to take down the cameras. As we understand it, anecdotally, a part of this had to do with cost, the cost of having people go through the tapes, keeping the tapes appropriately stored, if, indeed, you're going to form a database, and all that kind of thing. They did that, and they are willing, we understand, to share that with other law enforcement agencies. So, we don't have that, but you might be able to get it, if you wanted it. And the other part that's also sort of anecdotal is that following up on what Wade said, there's a convergence of systems, so, just because it's a camera involved doesn't make it the same.

So, if you take this "sueveillance" article that I told you about in the Popular Mechanics, we have the cameras that went into the police cars, and the police wanted to put the cameras in, because, in part, they were being accused of having problems at time of arrest, and so on. When you put together the camera in the police car, the camera at the police station as you're being brought in, and then cameras when you're taping, you know, interviews and so on, you have this interesting tracking that's worked in the reverse way, which is, it was more like a Freedom of Information transparency having to do with the police forces. Interestingly, both the public has accepted that and the police have accepted it. So, there may be times when, Wade and Clive, there are very -- at least point-specific places where everyone could agree that the cameras might be useful.

MR. NORRIS: Can I make one comment on that, which is perhaps rather surprising? In London, an experiment was run to put cameras into police cells. These police cells had integral sanitation, and there was no privacy screening mechanism to screen the image that the custody sergeant could see. What was interesting is, the research that was done on the people who were in the cells, actually a lot of them seemed to think that if it protected someone else, then it was worthwhile. And one of the things that was worried about in this particular station was the police assault. One of the key things was, though, that the police who had to watch this hated the system, they found it really uncomfortable, they didn't like it, and so forth. So, there were these peculiarities about what people will trade off in certain ways.

MR. SOFFEL: My name is Dan Soffel. I'm with the Illinois Emergency Management Agency, but I formerly was with the city of Chicago. And I guess my question for Clive, and maybe even for the panel, is -- certainly, it might be better to have a police officer on every corner. The problem is it's a resourcing issue, as it always is. I was troubled, a little bit, with your comment, particularly about the gunshot detectors, because I know that, in Chicago, we use

those integrated with CCTV in certain areas of the city. I think that they're an effective way to deploy scarce resources. I mean, we have police officers in those beats, in those areas, working those places. But the ability to not have to wait for the 911 calls to come in, but to actually take the data and deploy the officers in the best direction, looking for the best possible suspects or witnesses, it seems to me to be a reasonable way to use CCTV, in conjunction with other sensoring devices.

MR. NORRIS: Yes, maybe. It's the first I've heard of it. But, I think, as a model, would you still not say that having a citizenry that, immediately hearing a gunshot, would pick up the phone and ring the police, is the preferred model?

MR. SOFFEL: I guess my thought is, even if it's preferred, the data lapse between the time someone picks the phone up and I get the information in there, as opposed to having the information from a camera that can actually move and target onto the area where the gunshot came from, that's a whole lot faster, and I'm losing critical seconds, critical minutes, in terms of deployment of resources and assets to get to the scene it needs to get to.

MR. NORRIS: Well, then, in which case, a complementary system, fine.

MR. DEISMAN: If I can jump in on that one, for a couple of reasons, but mainly because I think the discussion here illustrates one of the key factors that's responsible for the expansion of CCTV, and it's called the precautionary principle. It's this idea that it's better to err on the side of caution, better to be safe than sorry, and it, kind of, has this logic associated with it, where it seems to provide a kind of wisdom, a kind of policy advice. While we would like to have some kind of failsafe, in case students -- or in case citizens don't actually call in, that we'll have this other system. It seems to provide a kind of wisdom and advice, in terms of policy choices, but it doesn't, actually, because every policy choice you make also creates additional risks. This is a key insight from an American legal scholar named Cass Sunnstein, who says that the precautionary principle actually -- in making these choices, we create other additional risks; one of them is that we deprive resources from other key police areas; another one may be that we create a fantastic privacy threat; another one is that we create this massive volume of data, data doubling, that's also available or in circulation, et cetera, et cetera. So, I think that's the sort of slippery edge of the slope there that we end up sliding all the way down to the bottom of.

MR. SOFFEL: I guess, only by way of response to that, I would say, if you simply did that, and simply thought you were going to set up cameras all across your city, and simply use them for that system, as opposed to an integrated system of patrol, where you're utilizing that technology in certain areas where you've got problems, where you're looking for specific issues, where you've got high gang crime, high crime areas, those sort of things, I think that you can do it in an intelligent fashion. If you're simply looking at it, and divorcing it, and saying that, this is the only solution that we have, that we can use to prevent crime and disorder problems, that's correct. If you use it as one tool of many, it's a good thing.

MS. BALLARD: Well, we have a law enforcement panel that's coming up after lunch, so hopefully all these questions will continue. Now, please, last question?

MS. FRANKLIN: Hi. Sharon Bradford Franklin, with the Constitution Project. Both the morning panel and this panel, all the panelists have seemed to agree that it is critical to establish, "what is your purpose? why are you setting up the system?" beforehand, and then to try and design the system to accomplish that purpose, which makes a lot of sense. Here in the United States, it seems like a lot of jurisdictions that are setting up cameras are doing this with DHS grants, and that's skewing the cost-benefit analysis, if you will, thinking through, "do I just want more cops on the street, or do I want other lesser technology that's less expensive", because the money is available for the video surveillance.

I'm wondering if, in your countries -- in Canada and the U.K. -- if you have a similar dynamic. Maybe the U.K, the cameras are already all over the place, but maybe in Canada, where you still see municipalities coming to the decision new, to set up systems or not, whether they are going through more of a, "what is the purpose", and focused determination, and if you have a similar pool of public funds available, whether it comes more with strings to force that kind of cost-benefit analysis.

MR. ANDERSON: Certainly, we had an example of a type of skewing, that's a real-life thing, is that we had a municipal transit group, and they had had some problems with attacks on drivers. And what they wanted to do was -- and, in fact, a driver had made a particular complaint, the organization wasn't protecting them, go off to a labor relations board, and so on. The labor relations board and the union, both thinking that putting in cameras by the drivers might be a helpful solution. So, we're not talking about terrorism, we're not talking about general policing, we're down, now, to a different, more specific kind of thing. But they didn't have the money to do it. And so, then along came the potential for some money that was really associated along the lines of terrorism, and so on, and the notion was, "gee, if we had that money, could use it for the cameras, it would solve this labor relations problem." And so, it was an interesting kind of flow-through of idea and of money.

MR. NORRIS: Can I just add, I think the similarities with Britain and the U.S. are actually quite intense, because we had a particular crisis in confidence in criminal justice in the early '90s which led to the massive expansion of public central government funds being pushed towards CCTV. And this seems to be the same that 9/11 has done here. If you look where CCTV hasn't really spread in public space in Europe, it's partly because it's been said, well, if you, as a police department, want it, you know, pay for it. And police departments in Britain have been very reluctant to pay for it out of their own budgets, which does suggest an interesting cost-benefit analysis going on there.

MR. DEISMAN: If I could jump in -- in terms of the Canadian case, and particularly Toronto, I think one of the factors which really has inhibited the growth of CCTV, but also in places like Montreal, is that there has been a very active sort of response from civil society, in

terms of groups that have risen up and been very incredulous about the benefits of establishing that kind of technology, and been very resistant to those kinds of encroachments on the right to privacy, and civil liberties, more generally.

MS. BALLARD: I want to thank the international panelists very much. This has been a great discussion. I appreciate your expertise.

[Applause.]

MS. BALLARD: We want to break now for lunch. There is a list of restaurants -- nearby restaurants -- in your information packet. Please be back here at 1:30. There seems to be a lot of information on law enforcement, and we have an exciting panel coming up at 1:30. Thank you.