DEPARTMENT OF HOMELAND SECURITY

PRIVACY OFFICE

PUBLIC WORKSHOP CCTV: DEVELOPING PRIVACY BEST PRACTICES

MONDAY, DECEMBER 18, 2007

Hilton Arlington

Gallery Ballroom

950 North Stafford Street

Arlington, VA 22203

PANEL ON DEVELOPING PRIVACY BEST PRACTICES FOR THE USE OF CCTV

McNEELY: Good morning. Can you all hear that okay? I'm Jim McNeely. I'm counsel for civil liberties programs with the DHS Office for Civil Rights and Civil Liberties. First, I want to welcome you, and I want to thank our hosts, with the DHS Privacy Office, for letting us free-ride in this great conference. I've been very heartened, so far, by the exchange of ideas. I've found that, even when I don't agree with everything that I hear, sometimes I'm convinced to change my mind, and, at other times, I'm forced to go back and reinvestigate why I think what I think about given issues, and it forces me to test my position. I sincerely appreciate that frank exchange of ideas. I think this has been a wonderful conference so far, and I look to this panel to be a capstone.

As an attorney, I tend to hide in the law. I tend to shelter in the law's thickets. But the problem is, in this particular area, the law only gets you so far. Dan Sutherland, on the first day, mentioned how we come to think about Fourth Amendment compliance as the be-all and end-all when it comes to surveillance issues. And we think that's sort of a mistaken way of thinking about things. What we've found, in practice, is it's fairly easy to reach agreement on most of the legal principles. It's a lot harder to come to agreement on policy issues and to come to agreement in the very difficult area of operationalizing the legal principles that we believe in. We seem to have a lot of disagreements in those areas.

My personal belief is that the solution probably isn't in a detailed statutory regime, but in building up good practices. Good practices become habits on the part of the operators. And the habits will govern the operators in routine circumstances and in dealing with circumstances that they don't foresee at the time the systems are set up. Good habits and having a good culture of respecting that vast area of freedom and human activities, good habits can govern the operators better than a set of rules can govern them, because they will do the right things. It can work better than any audit or any set of rules that we can apply from our heights at DHS headquarters. You know, from our heights, you'd think we'd know more about what's going on with the States and local governments, but we've received a lot of enlightenment from our panelists this week.

It's not easy work to come up with practices for our operators to follow. In fact, it's very hardwork. For that reason, I feel honored to be co-moderating this panel with Toby Levin from the Privacy Office, and I feel very honored that our guests are willing to share their opinions with us, and especially honored that they're willing to go out and do the hard work that preserving civil rights and civil liberties requires. They're willing to get out in the trenches to argue with us about best practices, and I want to sincerely thank them for it. This is very useful to us, and we look forward to working with them and hearing what they have to say, now and in the future, as we go forward.

I'd like to introduce our first panelist Nicole Ozer, of the ACLU of Northern California.

MS. OZER: Thank you. My name is Nicole Ozer. I'm the technology and civil liberties policy director at the ACLU of Northern California, and I work on the intersection of privacy, free speech, and new technology, splitting my time between our San Francisco and our San Jose office in California. In California we have over 100,000 ACLU members. In Northern California, we represent chapters that are all throughout Northern California --small towns, big towns, urban areas, also rural areas. Seems like we need to get a few more members around Clovis so we can get some more comments out there. So, I'll be working on that when I get back.

But, often I am the person -- when someone calls the ACLU -- many concerned members call the ACLU when they see in the newspaper that cameras are going to go up, or hear through the small town grapevine, and those calls often get routed to me and our police practices director, Mark Schlossberg, about their concerns with video surveillance. There are many, many community members that are very concerned about privacy impact, discriminatory impact, free-speech implications, and just the role of video surveillance and how it's going to play in a greater surveillance infrastructure.

I don't have a lot of time today. As you see, we have a huge panel here. We had some good comments in the earlier panel. But I did just want to note, if people haven't picked up our report that we issued earlier this year, "Under the Watchful Eye," issued by all three of the ACLU of California affiliates, and encourage you to read it. It lays out many of our thoughts

on video surveillance, issues of effectiveness, issues of impact on civil liberties. This is available both outside, also on our Web site, as well as many other accompanying materials.

We've been receiving a lot of calls on video surveillance. The last time we got a string of calls about video surveillance was actually in the late 1990s, when many communities -- most notably, Oakland, in California -- were considering video surveillance. In the 1990s, Oakland actually declined to install video surveillance. In their decision, former Oakland mayor, Jerry Brown, now Attorney General of California, decided that video surveillance was not something that Oakland should proceed in doing -- you can read his quote for yourself -- but they really did a thorough analysis, having public meetings, decided that video surveillance was not the solution, both for the fact that it wasn't going to be effective, was going to be expensive, and their concern about the surveillance infrastructure, that cameras were a part of a growing surveillance society, and what was going to happen to these cameras once that information was collected, where was it going to be used, how was it eventually going to be used. And there's not that much discussion this week, but we're here at a Department of Homeland Security meeting, and this money is coming from the Department of Homeland Security -- four different cities, not in a vacuum, operating within a whole infrastructure of Department of Homeland Security initiatives and other Federal initiatives, expanding surveillance of individual people in the United States, knowing much more information about us than we ever knew before 9/11.

In the 1990s, cities looked at video surveillance, declined to use video surveillance. Other cities who had video surveillance looked at the systems and declined to expand it, or actually removed it. So, what's happening now? In 2006, we did a public records survey, and we found that many, many cities were engaged in video surveillance in California. This is all detailed in our report– this is all late information now; a lot of this has now been updated, and that's available on our Website -- but 37 cities had some type of video surveillance, 18 had significant systems, and 10 were actively looking at deploying them. 18 cities had active monitoring; 11 -- only 11 cities that we looked at in California had even any kind of policy; most, not enforceable by law; most -- if there were policies, were only in the police department, and could easily be changed and modified and not enforced. And no cities – zero – big red zero – had done any kind of effectiveness evaluation about the money that they had spent or the money that they were planning to spend.

What's changed between the 1990s and now? What didn't change is that there's still no evidence that cameras prevent crime or make people feel safer. Some of the issues that were discussed yesterday by Clive and four others, also, there's been disappointment for prosecutions. What hasn't changed? We still have research about inexpensive and not as intrusive solutions, like lighting, which has been found to have a 20-percent average reduction in crime, including violent crime; also, community policing --that these things have had an impact. What hasn't changed? The impact on privacy and free speech and the

potential for discriminatory practices. Actually, it has changed; it's gotten more extensive. With better technology growing every year since the 1990s, with more integration of databases, with more issues that are happening from the Federal government, including things like fusion centers, there's more surveillance infrastructure. And some things have changed since the 1990s. Most notably, 9/11. But this change is not just because of 9/11. There are still many, many community members that are concerned about video surveillance and would like to have discussions and opportunities to talk about whether or not this is an appropriate strategy for their communities.

What really has changed since the 1990s is the funding stream -- the reason why many of us are here -- $230 million, to the tune of it. And with the change in funding stream, with the money coming from the Federal government, has been a circumvention of the normal types of public process that occurred in Oakland and occurred in many other cities where there was a thorough exploration of whether this was an appropriate strategy, there was a cost-benefit analysis, there was a vote by elected officials about whether or not the strategy should be contemplated. And much of this discussion in this public notice and this public exploration led to some of the rejection and discontinued programs in the 1990s.

So, that leads me to what I'm supposed to be doing up here. The ACLU's opinions on video surveillance and why we staunchly oppose video surveillance being used in communities is all in our report. What I'm doing up here is actually making recommendations about what should be happening, going forward, what the Department of Homeland Security should be doing, what people in this room could be doing.

My first recommendation is that DHS should be showing fiscal responsibility and policy leadership. My co-panelist up here talked about "Joe Sixpack." I believe DHS has a greater duty than the average Joe and Jane, looking at what actually is effective, in terms of policy, and how our taxpayer money should be used to better protect us. I would definitely say that there should be an effectiveness study of existing programs and a civil liberties impact assessment done. It's very good that there are organizations like the Urban Institute and the Samuelson Clinic that are working with cities to engage in effectiveness studies and cost-benefit analysis, but there really needs to be leadership from the Federal government, who's giving this money, to see if this is an area where our taxpayer dollars should be directed.

My second recommendation is that DHS needs to be showing leadership to restore the proper process. Much of the process of thorough evaluation and planning, which was discussed yesterday -- almost everyone on every panel discussed the need to have proper planning. Proper planning often does not occur when there is not actually a public process, and a process where elected officials and the public and the police department and all the stakeholders involved come together and discuss thoroughly what it is we're trying to accomplish, why we're trying to accomplish it, what resources we have available to us, and that proper process really needs to be linked to the grants. Most importantly, that public

process --public notice, impact assessments, and authorizations by votes of elected officials -- must occur before they submit a grant application. People in the community should not be learning that cameras are going up by reading it in the newspaper when the money has already been obtained, when people in the police department or other officials in the city have applied for grant funding without any kind of public discussion. So, that absolutely needs to be submitted before a grant application.

There should be an opportunity for public comment to DHS in relation to the applications for video surveillance grants. I haven't heard anyone -- there's been a lot of talk about public process happening in the cities, but I think that DHS should actually know what community members think about their cities applying for video surveillance grants, both good -- many people on the panels have said their community members are raving about the system. DHS should know that. DHS should also know if community members are very concerned and don't want the system. Also, a public process after the grants are received to determine placement and to craft enforceable standards, standards that actually have a rule of law and can be enforced. In San Francisco, some of our work led to one of the only enforceable standards in California. But even the city got that standard wrong. There was a notice requirement, which you think would be one of the easiest things for a city to do -- put up signs, saying, "we're contemplating putting up video surveillance here." We had to go back to them and actually read them the ordinance and say, "this is what your ordinance says. This is what you're supposed to be doing. Do it and if you don't do it, we're going to go to the police commission and have them renotice all the cameras," which the police commission actually did, and also, evaluation and public reporting post-installation of the cameras. These recommendations, I think, are good for DHS, they're good for the cities, and they're good for the public.

Pre-funding, there's a whole list of recommendations that we have. These really just resurrect the traditional budget process, whereby normally a city, when they were seeking to have video surveillance, would try to obtain budget funding for the system, and it would go through a public process. This really just resurrects that public process that existed prior to DHS being the one funding these systems. Why is resurrecting this public process good for all of us who are in this room? I think that it's good for DHS because it leads to better planning and structure. Cities that are actually engaged in a public process are more likely to be able to be successful and achieve the public safety goals that this money is supposed to be targeted to. It's also good for cities because I can tell you that community members that read about these cameras right before they go up are not happy people. And the money is tied up in public meetings long after the fact. When you're hoping to get up the money, and you're on a certain budget cycle, and then comes the community members, and then comes the ACLU, and then comes the minority groups, that is not the time when you should be starting to discuss these issues. I think there's a much stronger chance for success if you can start this planning earlier.

It's very good for the public, because then we can actually have a balanced discussion of whether these are really the strategies we want to employ, and that there are serious consequences for the public to video surveillance. I think it's very important that the public feels that they're listened to, both by the local entities and also by the Federal Government. As I said, during the grant application, I think it's very important that there's an opportunity for public comments, because DHS should know the opinions of community members. I also think that it functions as an audit. If there are public processes that you're rolling down with the grants, you can then hear from the community members if they feel that the city is actually complying with those policies.

After funding and before installation, use public notice and public meetings to discuss where the cameras should be, how they're going to be used, and legally-binding ordinances. Then, finally, after installation, the enforcement of legally-binding ordinances, an evaluation about use and effectiveness should take place on a yearly basis or before additional cameras are installed. I think this evaluation should be submitted to DHS, elected officials, and also made available to the public. Of course an independent entity should be involved in the evaluation. I think that this is good for DHS because it builds best practices for how to structure these systems in a way that's most effective and minimizes negative impacts. I think it's good for cities because a lot of people in here have learned from each other just through this event. Imagine if there was actually a databank of what's worked for cities and what hasn't worked for cities. I think that would be very useful in terms of efficiency and it's good for the public. This is about transparency, it's about accountability. This has an impact on civil liberties and it's costing taxpayer money. I think that the public should know how and whether a system has been effective and what the impact has been. So, with that, you can read a lot more about our thoughts in our report. It's also online. I look forward to your feedback.

MR. McNEELY: Thanks so much, Nicole. The next speaker will be Sharon Bradford Franklin, who is senior counsel with the Constitution Project. You may have recognized her pamphlet, which is available in the lobby.

MS. FRANKLIN: Thank you. The Constitution Project, for those of you not familiar with us, is an independent think tank whose mission is to promote constitutional safeguards. We do this mostly by pulling together bipartisan blue-ribbon committees to confront various issues and working with them to develop consensus recommendations for policy reforms.

Relevant to today's presentation is our Liberty and Security Committee, with whom I work a lot, and that committee was developed, after September 11th,to try and develop policy recommendations on how we can maintain our civil liberties as we simultaneously work to improve our national security. That committee came out with this report, last year: *Guidelines for Public Video Surveillance.* We did not have, unfortunately, enough of them to make them available to everybody, but you do have in your packet a summary encapsulation, in the

form of some PowerPoint slides, and, at Toby's recommendation, this is just a handout. You won't be seeing the slides as I speak.

The very first slide tells you where you can find the report on our Website, where it's available as a PDF, and so, I'd encourage you to have a look at that. Those of you in the audience who are with State and local governments or police departments that are considering, or already have, video surveillance systems, I would love to be able to also work with you, make copies of these available to you, if you want to see me afterward. But today I will summarize what is in our guidelines because these really are conceived as a set of very practical recommendations for State and local governments that are establishing video surveillance systems, or considering it, and the steps to go through. I'm going to talk, just very briefly, about how the guidelines are structured, but then really spend more time putting these in the context, as Toby Levin asked, about the fair information practice principles, because the DHS Privacy Office really does focus a lot on the fair information practice principles, and to talk about how these guidelines really do help communities to implement those.

Our structure, as you will see in the handout, is in three parts. The first part just lays out a series of core principles that govern the creation and design of the system -- up front, what you should think about. These are things that a lot of our panels have talked about, and that I will get to in the context of the fair information practice principles, but including, most notably, making sure you have a clearly articulated law enforcement purpose before you ever go about setting up any type of system.

The second section outlines two types of publicly accountable procedures that communities can rely upon in order to go through this process of setting up a system. A lot of the process recommendations really are very similar to what Nicole was just talking about for the ACLU, in terms of involving public comment and having a full public debate beforehand to really think through all of these variables. The only point I did want to just mention is, we also recommend, separately, a different procedure that can substitute for a temporary system. When you're not talking about putting up the cameras that are going to be a permanent part of your public infrastructure, but if you have a specific need for a targeted law enforcement investigation, you may be able to go through a procedure we recommend to substitute judicial process and the oversight by a judge or magistrate to, sort of, substitute and provide that accountability.

And the third section of our guidelines is a set of principles and rules governing the use of systems once they're in place, and making sure that they are then used effectively.

Now, I just want to walk through the fair information practice principles quickly. The first principle is the principle of transparency. And there, two key parts are, one, using the publicly accountable set of procedures to set up your system. I'll defer to other panelists who have really talked at length about those kinds of recommendations, such as the ACLU

mentioned, that we would also support. And the second is using signage to alert people to the general location of cameras. There may be considerations where you don't want to put the sign exactly on the specific camera, because perhaps that won't help you catch the people that you want to catch, but, generally, the notice is for the deterrence, as well as for the public transparency, that a particular area is under surveillance.

One other aside here. In the slides in your packet, I do have cross-references there to the pages of our report where that is discussed more fully. I neglected to mention that at the back of our report is model legislation. That model legislation is something that we developed in connection with a prior panelist, Deirdre Mulligan and her clinic at University of California at Berkeley, and my co-panelist Jennifer King, also represents them. That legislation, at the back of our book here, is designed to provide a model for communities, hopefully to enable them to enact these guidelines into law with ease, and just cut-and-paste, and adapt, and make that as practical a tool as possible. In those slides you have in your packets, there are cross-references to the relevant sections of the model legislation that would help you to implement these.

The second fair information practice principle is the principle of individual participation. There again, these are ones that have been covered a fair amount by other panels and other panelists. But, including an opportunity for public comment is really critical as part of your procedures to establish the system. Another way in which this comes up later on is that the individuals have rights in this information. In the video surveillance database, if you are retaining footage, and you have identified, maybe with a metadata tag, someone's name, who this image pertains to, those individuals may have rights to request a report listing all those instances in which they are identified with their image in your database. So, that's another thing for communities to think through.

The third principle is the principle of purpose specification. I've been really pleased to hear panel after panel emphasize this because this really is critical, and this really is our first core principle of design, that these systems really should only be set up to further a clearly articulated law enforcement purpose. Just from the articles I've read in the newspaper, it seems that too many communities are just looking at this as a tool to pacify the public, and not thinking through, "what is this going to be targeted for?" and "what is this going to achieve?" Everything follows from that, from whether you should do it in the first place to how you design your system to really achieve that purpose. So the corollary to that is to ensure that when you design system it's going to be capable of effectively achieving that purpose.

The fourth principle is the principle of minimization. This is one I will spend a little bit more time on, because there are a lot of ramifications for this, for how you might go about designing a system. The first aspect comes up in your deciding whether you need this or not, whether video surveillance is needed to accomplish whatever the specific law enforcement

purpose is, or whether better street lighting would do the job, or more cops on the street. A lot of other panelists have talked about that. The second is, when you design your system, you want to minimize the impact on constitutional rights and values -- and these include things like privacy, freedom of speech, freedom of association, and equal protection that need to be balanced with your system and designed into the system. Let me give you some examples of what this might mean in practice. Let's say you have a camera system that you have set up, and you pick locations because you actually have public infrastructure -- we heard the Park Service, yesterday, talk about our national monuments that we need to protect. So, you have cameras set up to protect various national icons that might be subject to terrorist threat or other types of threats. If you have some type of public building that is next to an apartment building, those cameras should be focused on the building that is your subject of your protection, and you don't need to be able to pan, tilt, and zoom, and look into the windows of the apartment building next door. Fairly straightforward example, but not always followed in practice.

Another example of what "minimization" mean is if you have a camera system set up to protect against traffic problems-- a public safety purpose, and so you have it at certain intersections that you know are subject to a lot of traffic incidents. Well, your theory here is, you want to be able to send out your officers to help stranded motorists, to assist in an accident, send out your ambulances, so forth. Well, that system doesn't need to be equipped with facial recognition technology. You don't need to be able to identify the passengers in those cars; you just need to know whether you need to deploy an officer to the scene. A final example comes up in the context of First Amendment protected activity, of political demonstrations. And here, this may go to your retention policy. The example came up in Washington, D.C. when they were setting up the cameras initially, it was just on the Mall, trying to make sure if there was going to be a non-peaceful demonstration, if they needed to deploy officers. They weren't even recording. Then they said, "oh, well, we have these cameras here, maybe we should go ahead and record. It's not that big a deal if we have these cameras there." Well, you're going to know right away after you have deployed your officers, maybe there was an incident -- you're going to know right away whether there actually was some type of incident that rose to a criminal level and whether you need to retain that footage for that purpose. If not, there is no reason whatsoever to retain this footage of political activity and First Amendment protected activity.

The fifth fair information practice principle is the principle of use limitation. Several points there that come up in our guidelines. One is to prohibit, to the extent possible, the sharing of the data with third parties, including private litigants, and to restrict the sharing, to the extent possible, with other government entities. The second two points that I wanted to mention is the concept of requiring additional specific approvals for use of your system for things that are more intrusive. One of the panelists on the earlier panel, Marc Blitz, mentioned that there are certain technologies, like automatic tracking and automatic

identification where you might have a digital database of all your networked cameras, and you might one day have the ability with biometric identifiers to tag somebody and trace their movements throughout your city, throughout your database, and compile a digital dossier. Well, just because that technology is there doesn't mean that it should necessarily be used in any given case. That's the kind of thing that might be very helpful if you actually had a suspect that you were trying to track down, if that data is there. So that's the kind of thing where to track normal police practices requires something like a search warrant, probable-cause shown to a magistrate that you should be able to go ahead and do that search through your database for all those instances of that person. You should have some reason to track that person down.

Similarly, we recommend that in the case of using the footage for what we call a secondary purpose -- we've talked a lot about your system being designed for a purpose. Well, it may be that you've designed it, for monitoring violent crime and really tracking that down, but it turns out that somebody comes to you and reports to you that they were the victim of a pick pocketing, and they were in an area where they saw there was a camera, and so, they think you might have some footage of this. You would then have to make the kind of showing of probable cause, or so forth, to go back and look at that footage, because you know it might show something for a legitimate law enforcement purpose, even though it's a different one. In this case, perhaps a lesser one than what you set up your camera system for. So, the recommendation isn't to tie your hands so you can't use it, but that you shouldn't be able to go on a fishing expedition just looking for what else might be on there.

The next principle is the principle of data quality and integrity. There we have had a fair number of panelists talking about some of the possible safeguards that you can use, such as digital watermarks for the use of stored video surveillance data, as well as safeguards for personnel who have access and the need to work with this system Finally in this category would be establishing a data retention policy that recorded footage lacking any evidentiary values (which can usually be determined in a pretty quick period of time) will be routinely destroyed on a set schedule. The next principle is the principle of security. That would include things like providing sanctions against misuse and abuse of public surveillance systems, as well as remedies for people who may be harmed by those types of abuse and misuse. Also included in the principle of security is the creation of technological and administrative safeguards that actually use the technology as protective of rights, not just for the power of the cameras, but techniques such as digital masking of people whose images are incidentally captured and aren't actually your criminal suspects.

The final principle is the principle of accountability and auditing. And, there again, we, like many others, recommend periodic audits on a routine schedule. The final thing we've put under this category is for the use of privately collected video surveillance data, and that's something that's come up, as well. The recommendation is that even if you obtain this

because somebody turns over the footage from the ATM camera or if you have a more routine use, as we've heard of with Clovis -- once that data comes into the government hands, it should be treated with all the same protections and safeguards as if it had been recorded initially on a government-run camera. So that is how the guidelines can fit under these principles. I'll be happy to take questions later.

MR. McNEELY: Okay, thanks very much, Sharon. The next speaker is going to be Sophia Cope, who is a staff attorney with the Center for Democracy and Technology.

MS. COPE: Thank you, Jim. Being on the last panel, we were actually given a charge to drive home some very key points and to bring out some important themes. So I'd like to really drive home a couple of things. The first is what localities should do before any cameras are purchased. Secondly, I'd like to give some specific guidance to DHS. I agree with everything that has been said in terms of operational best practices, but I think DHS as an agency really is looking to figure out what they can do under their authority. And so, I have a few suggestions.

In terms of what localities should do before cameras are purchased, give a more philosophical or bigger-picture perspective. CDT is a public-interest, nonprofit, public-policy organization, and we focus on the civil liberties implications of technology. We primarily focus on free speech and privacy. We try to weigh in on any technology issue that implicates those rights. While we haven't specifically focused on CCTV, we do work very extensively on issues related to identification cards including the REAL ID Act, for example, and other identification systems like the electronic passport and the proposed passport card that both use RFID technology. We generally are concerned about the increasing requirement to show identification and to identify yourself either in the offline world or online.

Many people, including Deirdre at UC Berkeley, have mentioned sensor networks. Again, RFID can play into that, but there is also sound, vibration, and smell. At CDT we work a lot with electronic surveillance, more pure, traditional government wiretapping, and also more modernly, tapping of the Internet. We work a lot on the whole NSA/FISA issue. All of this is related to the digitizing of information, the electronic storage of information databases, and how all of this technology has allowed for greater ease of collecting information and sharing information. I wanted to give you a bigger picture of what we work on at CDT because we are creating a surveillance society. Whether we like to admit it or not, from our perspective, CCTV is just another brick in the wall. The reason I really want to hammer home the analysis that should happen before CCTV systems are bought is precisely because CCTV is another brick in the wall. The preliminary analysis-- the need analysis, efficacy analysis, and cost-benefit analysis--really is important to do up front. Do it sincerely and in good faith while not caving to public pressure and not having dollar signs in your eyes because you're getting government money. Do it thoroughly and to do it in a way that really benefits your community.

So, what should a cost-benefit analysis look like? And, again, this should be done beforehand. We get very frustrated at the Federal level -- and not to dig on DHS too much -- because a lot of impact assessments and cost-benefit analyses happen after the program is already planned and is about to be rolled out. It's just this procedural hoop that the Federal agencies go through, and it really doesn't inform the up-front decision making at all. From a process perspective, it's a major issue, it's a major problem, and it shouldn't be just a procedural hoop to jump through.

So this has been mentioned before, but I think it's really important. It's not just highlighting what the program goal or problem that's to be solved. It really involves what is the specific goal or problem that exists. Terrorism -- preventing terrorism -- that's really broad. Violent crime is very broad. But if you say, "we're having vandalism on this particular street corner," that's a lot more specific. If people are running red lights at this particular intersection, that's very specific. And again, other people have mentioned that there are non-crime problems that potentially – and this is the benefits analysis –could be solved. Can we have better crowd control? Can we manage traffic better? And, again, this all goes to, is CCTV needed and what's its efficacy?

So you identify the specific problem and focus on specific locations within your jurisdiction. The real heart of the efficacy or the need analysis is, of course, whether or not CCTV will actually help solve the problem or reach the goal. Something I want to highlight that has come up in these last 2 days is that there is a difference between prevention and deterrence, in terms of crime, and investigations after-the-fact having evidence for prosecutions. I think that distinction is really important in trying to determine when CCTV's going to be effective for you.

That's another thing that's come out of this conference, is that there are so many lessons to be learned by other jurisdictions that are further along in doing this. Academic studies of effectiveness, and even anecdotal studies of effectiveness, I think, inform the analysis. As the international panel mentioned, the studies have been fairly dubious about the effectiveness of CCTV.

Of course the financial cost is very straightforward. We heard yesterday that Baltimore has spent $17 million on CCTV, which I thought was astounding. And, as has been mentioned, if you're getting money from the Federal government, that number may skew your analysis because it's essentially free money and it's not coming out of your local coffers. But still, that's a lot of money that perhaps could be used in different ways. Other financial costs that people have talked about incorporating into this cost-benefit analysis include maintenance and auditing costs, and even, maybe, costs of litigation and other things that aren't anticipated but should definitely be factored in.

Then there are the intangible costs, which from CDT's perspective, are the most important. That is the meat of what we've been talking about these last 2days. These specifically are the

privacy and the civil liberties costs. The core of this problem is that video surveillance, and everything else that could be attached to it, does change the relationship between citizens and the government and can facilitate an abuse of power. The legal panel and other panels have mentioned that. In terms of First Amendment rights the key question is whether people are going to be chilled from doing something that they're constitutionally free to do?

In the Fourth Amendment context, the police can't randomly walk up to people and say, "papers, please." I'd like to think that Americans have prided themselves on the fact that we don't live in a "papers, please" society. But again, ,if there's video surveillance and there's facial recognition or some other way to identify people without probable cause, or at least reasonable suspicion, or even judicial review in the form of a warrant or something like that, the "papers, please" environment becomes a reality. Then there's the issue of social conformity, so it's not deterrence of crime, but, "okay, I've been tapped." I'm going to get to the recommendations for DHS.

Social conformity; video surveillance is not just crime deterrence. The cost-benefit analysis should be applied to the specific proposal that the local jurisdiction has in mind. So it's what locations, what street corners, what neighborhoods, while thinking how many cameras, and what are the capabilities of those cameras? Is there going to be zoom? Is there going to be sound recording, panning/tilting, facial recognition, iris scans, gunfire detection? Storage retention is a huge issue. Active monitoring or automated monitoring, live feed? Can the police talk to the people they're monitoring? Are they going to have access to other databases? Is there going to be a wireless interaction? There might be some security issues there.

The final aspect of the cost-benefit analysis is what alternatives are there to solving the problem? If we're talking about preventing crime–do lighting, foot patrols, community policing make more sense? Root causes are really important, too. If you have a pot of money-- and I know there are some restrictions with DHS grants, do you want to buy cameras, or do you want to, perhaps, have after-school programs, job creation, sports, urban redevelopment, affordable housing, drug treatment programs? I also want to give some concrete suggestions for DHS.

There should be a rigorous application process. There already is a rigorous application process for homeland security grants, but I really think there should be one for CCTV, specifically. I think the problem that we're seeing now is that CCTV funding is lumped in with these billions and billions of dollars of homeland security grants; and there's just one kind of line item in the grants, not a whole separate application process for CCTV.

Our main thesis is that there really should be mandatory privacy and civil liberties, and even security, conditions attached to these grants. Currently, the homeland security grant process already does require investment justification. There's a review of effectiveness. The grantees already have to make promises to avoid conflicts of interest, to follow certain Federal

antidiscrimination laws, and even environment protection laws. There's equipment, technology, training, evaluation, and contracting requirements. So, there's already these requirements built into the bigger homeland security grants. I really think that similar requirements specifically for CCTV and the issues related to CCTV should be incorporated into the grants.

OMB, the Office of Management and Budget directs the grant making process, and there's already OMB guidance and requirements. OMB already requires a cost-benefit analysis. It does say that there must be OMB approval for additional conditions. But I think DHS could easily work with that. There's already an OMB requirement that there be an after-the-fact evaluation of the results and the success of the project. I know that there's an issue, administratively, with the fact that a lot of grants go to State administrative agencies. But, again, I think DHS can specifically work with the SSAs to figure out how they can help with meeting privacy and civil liberties standards.

And, here is some practical advice, a few tips for DHS, and then I'll end. DHS can, of course, write "best practices" if they don't want to impose mandatory conditions on grantees. And, as Sharon said, they should be based on the Fair Information Practice Principles. And this is consistent with the DHS authorizing statute, which requires DHS and the Privacy Office to advance the FIPS throughout their work. There are a few practical things DHS could do: a model cost-benefit/efficacy/privacy/civil-liberties analysis -- DHS could create that for the local jurisdictions, as well as a model post-implementation assessment tool. Model legislation; I know the Constitution Project has a good draft. Model training curriculum. Training came up a lot– or the lack of training – and I think DHS could work with local jurisdictions and come up with a model training curriculum. Model public surveys. There's been talk of a lack of public input. DHS could easily come up with model public surveys to gauge public interest and concern before implementation of a CCTV program, and then to gauge public reaction once the program is up and running.

DHS can create a simple Website that's a clearinghouse for CCTV information, grant information, the grant conditions, if there are conditions, or the best-practices guidance, and all of these tools that I have suggested, existing best practices from nonprofits, information about what other jurisdictions are doing, studies of effectiveness, and vendors who offer privacy-protecting features. All of these things can be in a Website clearinghouse that DHS creates to help its grantees. And this has been mentioned, too -- a centralized way for grantees to share information, to share horror stories -- which came up yesterday -- and also to share successful privacy and civil liberties protections.

So, there are a myriad of things that DHS can do as an agency to show leadership here. The panels yesterday -- in fact, I think, the law enforcement panel -- they were very receptive to DHS guidance and tools, but actual conditions on the grants. They said, "hey, if it's tied to Federal money, we're going to do it." So, I think that where there's a will, there's a way.

And, in this case, when we're dealing millions and billions of dollars, DHS has a lot of room to really show leadership in this area. Thank you.

MR. McNEELY: Okay, thanks very much, Sophia. That's a great example of specific suggestions which we can take and consider. I really appreciate the kind of effort you've put into that. Our next panelist is Jennifer King. She's a research scientist and an information specialist at the Samuelson Law Technology and Public Policy Clinic at UC Berkeley.

MS. KING: Hi. I was asked to look at these guidelines as a technologist. And so, that's exactly what I did. So, I went through them, and, I think, overall, they do a good job of not mandating a specific technology to solve a lot of these problems. That's one of those issues that, when you deal with technology, industry is often very concerned with, that you're going to mandate them into using a specific type of technology and basically check innovation and tie you to something. Instead, I think these give a lot of room to grow without making a specific recommendation that might become obsolete over time. I think there are many things in here that are prescriptive, but they're not necessarily technical prescriptions, but they can be solved by using technology.

And, going through some of the principles and rules, number three in here is that individuals may be tracked or identified by a public video surveillance system only pursuant to a warrant. That's the type of thing I could imagine using a technological solution to actually enforce. "Employing technological and administrative safeguards to reduce the potential for misuse and abuse of the system," again that's a clear call for doing things like logging, access control, and making, basically, a very clear audit trail. That's something that software can absolutely do for you.

Also, we have "prohibit, to the extent possible, sharing of public video surveillance data with third parties." That's something where, if you're concerned about your actual users of the system, you can do some very simple things, like making it impossible to send e-mail from the actual control room, for example. That's one simple approach. Or just making it impossible to make copies of tapes or files without a supervisor actually approving it. These are all things that the software system could essentially do for you. There was only one thing in here I found a little problematic, and one thing I think is actually omitted from this set of guidelines.

One of the things I found problematic was in the principles of individual participation. I think this is actually in the model legislation piece-- where they note that, "individuals should have the right to request a report listing instances in which they appear in video footage and are identified byname, and should have a reasonable opportunity to amend that data if it contains errors." I find this one a little difficult, because I'm not optimistic about the state of most police data-collection systems. I am imagining that when video surveillance technology is incorporated, it's being brought in on top of an existing system, and that you're not starting from scratch. This is the type of thing where I doubt that, even today, if my

name appeared casually in a police report, that someone could do some sort of search and be able to find that sort of thing. So, this is one of those -- it's a little bit nit-picky, but it's the type of thing where I think it's a very important principle, but, in terms of a technology solution for it, it might be a bit problematic today, just based on legacy systems, for example.

One of the things I thought that was omitted when you look at the principles of security, there's certainly a lot of concern put towards insider threats to the system, but one of the things, I think, that really should be explicitly called out is external threats. And by that, I really mean looking at the security of the network. This is really important, as most of these systems are moving away from wired systems to wireless systems. There's already been a documented case in Europe -- I think it was in Austria -- where hackers were able to hack into the wireless network and redirect the camera feeds. And so, I can imagine, in smaller jurisdictions, where there's less cognizance about security, people, having access controls on the wireless network, but using a really simple password, or not even changing the default password, for instance. So, calling out network security is one of the critical pieces of one of the security principles I think that's probably missing from these guidelines.

Finally, I just wanted to note that having sat in the room with most of you folks now for a day and a half, it seems like we all think we're basically on the cusp of an explosion of surveillance systems in the U.S. I noted yesterday the representative from the International Association of the Chiefs of Police said that they were in the process of redoing their guidelines. I think that might be a great opportunity for that organization, or another one -- I don't know who else, besides most of the people in this room, are really focusing on these issues -- to really take advantage of, not only the wealth of experience that's across the Atlantic, but also from some of the cities that have systems, and have had them for a while, and are really maturing in their use in the United States, like Chicago, Los Angeles, Clovis, who's been here, and there are others not necessarily coming to mind right now. But there's obviously jurisdictions that have been putting this into place now for -- some as long as 5 years or more. It seems like a great time to actually bring together an either formal or information network of police professionals to begin sharing experiences with technology development and how they've actually implemented it.

But I would be bereft in not mentioning that I think if that sort of thing is to happen, that it's imperative that some other parties get involved, like maybe the Constitution Project, or at least advice should be sought from those of us who work in this field, rather than keeping it police-specific, to also make sure that you're considering it from all the different points of view you've heard over the last day and a half with regards to civil liberties and such.

MR. McNEELY: Thanks very much, Jen, that was good advice, and something I try to pay attention to as I listen to the operators, because the operators will often tell us how we can achieve our ends. In our experience -- I know, with privacy, as well -- the crux of the issue is reconciling people who have very abstract and noble goals with the people who have their

boots on the ground, and find out where we can match up those interests. Speaking of that, Chief Thomas Nestel, chief of police for Upper Moreland Township, Pennsylvania, is our next speaker.

MR. NESTEL: I was asked to review the comments that are presented today, and explain whether or not law enforcement professionals would be willing to accept those recommendations. So, I've been jotting down some notes. The ACLU recommends public involvement. And I agree. In Philadelphia, not only was the public involved, but they decided whether or not CCTV should be introduced to the jurisdiction. It was a ballot issue that was overwhelmingly approved. I believe that government hearings should be held in that jurisdiction to determine the process on how the cameras will be assigned. Where will they be mounted? What will the purpose of the cameras be?

When the Constitution Project suggests that there should be limited information-sharing specifically with private litigants, we couldn't agree more. We absolutely are very concerned about the divorce case, the traffic accident, all of those issues that are not why the cameras are being implemented. When it comes to sharing the information with other government entities, I think that we would pause there, because we would certainly want our partners in the FBI or in the State police or other law enforcement jurisdictions to have access to the information that we're storing. The issue regarding search warrants to go back into archived data, we would jump up and down, and stamp our feet, and say no, and put our hands over our ears. All of that data is from the public domain. There is little expectation of privacy. We're not violating any constitutional rights to gather it; nor are we, to store it. So, we certainly would be opposed to requesting a search warrant to look at that reasonably-gathered information.

Safeguards, absolutely. Encrypting, watermarking, chain-of-custody issues that law enforcement are very good at implementing and establishing and practicing. Audits, absolutely. I said yesterday that I believe that law enforcement can audit their system, but I also think that they would welcome an outside auditor to further bolster the faith of the public in the system that we have. Cost-benefits analysis. The Center for Democracy and Technology suggests that. Really, really difficult to do. We struggle, in the homeland security realm, to determine a quantitative assessment of when we're successful in protecting a critical infrastructure location. It's extremely difficult to do, and I know that there is constant debate about that now. So, their views are pretty holistic. They're very general. I tend to drill all the way down into the police world, and I'm going to repeat something that I said yesterday, that over 70 percent of the departments that I surveyed that have CCTV do not have a written policy. A written policy is the absolute baseline for any police operation. You have to have a written policy. And with a written policy, you have to have supervision. In order to run a CCTV operation, there should be supervision, and there should be constant

supervision. A sergeant, a lieutenant, some supervisor should be present at all times when the system is running.

The third biggest part is training. Again, in the survey, I found that very little training, other than on-the-job training exists; and no follow up training, except for one jurisdiction, a yearly refresher, exists for camera operators, control-room employees, supervisors. It has to be an ongoing process. It has to be a message from the agency head that this is an important function and that civil liberties are protected.

MR. McNEELY: Thanks very much, Tom. That highlights that linkage between the Constitution and our policies, practices we put in, and the implementation. Training is, we've found within the Department, in some cases, that final implementing step. It's that gap that you have to cross. Our next speaker is Clive Norris. He's a professor at the University of Sheffield in the United Kingdom.

MR. NORRIS: Thank you. Some of you who were here yesterday might find it rather surprising that, with, I think, the exception of maybe one issue, I would find it very difficult to have disagreed with the chief of police, here. I want to give you some reasons why that is the case, from the British experience. Well, actually, let me start by saying where I think you should start this debate because in Britain, 1994, when CCTV came into being, we were actually in a similar place. There was really no legislation, there were no guidelines, perhaps the Data Protection Act applied, but perhaps it didn't. It wasn't really clear at that moment. And, actually, one of the things that I think is really quite important here is that there is a document now, the Constitution Project document, which I think sets out a basis for having a discussion, and a very good basis for having it. There will be disagreement about it, particularly one was highlighted here, which was over the issue of tracking. I think that is going to bean interesting debate.

In Britain most public center systems are based around tracking facilities, about being able to monitor someone as they move through space. As I talked about yesterday, the database of drivers' vehicles movements will enable that tracking of 50 million vehicle movements a day, to be carried out retrospectively for 2 years. So, tracking is an integral part in Britain. I think that's going to be an interesting debate that needs to be had. I don't know how it will be resolved. But I think the important starting place is to say, "well, when systems are put in place," and let's say America's at the beginning since there may be now an expansion of CCTV across a whole range of cities and new spaces, "getting the dialogue about civil liberties and privacy impact assessment at the beginning, before systems go in place, is really important." That way the people who are responsible for developing the systems actually start to engage with these issues and take them onboard, not when it's too late or as an afterthought, but as a fundamental principle. I think that would have really helped in the British context. If we go on, specifically, to the British context of regulation, as I say, CCTV

developed in the absence of regulation, but it was bought under the fold, predominantly, of the Data Protection Act.

Now, what's interesting, and interesting about Britain, is, on one hand, there is always a tension between regulators and implementers. One of the things that's happened in Britain is that the implementers, particularly of the sorts of CCTV projects that are being represented here, the big city-center systems, which I suspect are models of that type, they are very concerned about the lack of regulation. One of the things they're concerned about is that, actually, there's a danger that the bad will drive out the good, that their reputations will be sullied by poor operators across the country by the non-regulation. And let me just read what the chair of the CCTV Users Group wrote. He wrote about the Information Commissioner's Office, "the information commissioner has inadequate investigative staff to ensure compliance with the Act. Only if complaints are made about the specific system will any investigation be carried out. We are also concerned that, whilst organizations are required to notify her of any CCTV system, this can be done by bulk notification of all the organizations' data-protection obligations, and, therefore, no separate record which can identify every CCTV system, and who is responsible for operating it, exists."

So, although you may look to Britain as a model of regulatory practice under the Data Protection Act, one of the problems is that it's actually been very weak. One way of seeing how weak it is, as I pointed out, of our survey, 78 percent of signage wasn't legal. How many people were prosecuted for not having legal signage? As far as we're aware, none. Indeed, how many people have ever been prosecuted around CCTV under the Data Protection Act? As far as I am aware, none. If you set up a regulator who has no powers of inspection, very few staff, then the guidelines they issue will have, actually, I think, an impact on those big city-center projects where project managers take them seriously, but it's not going to have much impact on smaller systems or rogue systems, and so forth. So, I think there's a real issue to be addressed there.

I think there are perhaps three key principles. And, as I say, I think a starting point for a debate is the Constitution Project's guidance. It looks very good. I would say that, given the way that the camera and our CCTV systems alters the relationship of the gaze of the State between the citizen, we have to think about that. I disagree with the legal judgment that says it is merely an extension of a pair of eyes. I would very much agree with the analysis that Deirdre gave earlier this morning, that you can't equate it like that. A video recorder isn't like our memory. We can't zoom in from 100 yards and see these things, and so forth. So I think we have to take that as a premise. If we take that as the premise, I think we have to say, when we enter a video space that someone's watching us, we have the right to know. We have the right to know that we are under surveillance. So, there should be signs, and they should be clear. Those signs should also declare who is responsible for a system. And this then relates to a separate issue. If that's the case, covert cameras actually are highly

problematic under that. I think one needs to think very carefully about the separate and the more intrusive and invasive nature of covert surveillance, as opposed to overt. And one, perhaps, needs to separate the two out. In English law, to some degree, that does happen.

The second key point that I would make is about disclosure--that where CCTV systems are put in place, they should have an articulated purpose -- and that seems to be public security, in the broader sense, the prevention of crime, detection of crime, prevention of terrorism, or whatever. In which case, the information that is received by those systems should not be disclosed for other purposes. I think this is a point that's been made about private disclosure to insurance companies, or whatever. That's what it was for, and that's what it should be limited to. The disclosure should be limited to the prevention and detection of specific crimes.

In Britain, one of the most celebrated cases around CCTV revolved around the local authority, who issued some footage of a man who had a knife, and they dispatched a police car to it and the man was taken away. Actually, what happened was this man was attempting to commit suicide. They released this footage to the media, and they released it because what they wanted to show was that this was good practice, that, actually, CCTV has helped, saved a life. What they failed to do, though, was ensure an adequate agreement with the media of how that footage would be dealt with. They did not disguise his face. So, this person's image, someone who had been very distressed, distressed enough to have tried to commit suicide, was broadcast all over national television, and then, for the next 5 years, a legal case went on about whether this had been a breach of some law or other. Eventually it got to a European court, who decided it had. British court said there hadn't been. This was before the Human Rights Act. But that's the sort of thing that no one had anticipated. This is when -- we heard yesterday, about the need to collect evidence of bad practice. Bad practice often reveals something that wasn't intentionally done badly, it's just, no one thought through the consequences. And, in Britain, that very much changed the way that most local authorities and CCTV operators actually disclose information. There's a lot less footage available now. It's very, very hard to get.

My final point is that if you look at the British experience and you know anything about regulation, if you have just bits of paper, some people will act in good faith and use those bits of paper and the guidance and have good practice. But you can't guarantee it. And, therefore, if you want public trust in systems, you must have some external oversight of them -- and that is one of the key weaknesses, I think, in the British system, is the independent audit cannot be done by the Data Protection Office unless they have a specific complaint -- and that, when you do that, the results of such inspections should be made public.

MR. McNEELY: Thanks very much, Professor. The next speaker is Barry Steinhardt. He's the director of the Technology and Liberty Program of the American Civil Liberties Union.

MR. STEINHARDT: There should be a short video.

[Video presentation.]

MR. STEINHARDT: Now, why did I show you that video, aside from its shock value? I showed it because I think it illustrates some of the dilemma that we have now. First, let me put this in some context. Where did that video come from? Some of you may know, there was a fair amount of surveillance around the Republican National Convention 4 years ago, and there was some litigation which the ACLU and the National Lawyers Guild brought challenging some of that surveillance. In the course of that litigation, there was discovery, of course, for the lawyers in the room, the ritualistic asking for information -- and what emerged was the essence of that story, which was a videotape taken by the New York City Police Department. And what was extraordinary about the videotape was several things. One, of course, was what you saw-- the abuse of sophisticated camera technology by police officers, police officers who were probably a little bored. Nothing much happened at the Republican National Convention. There were no terrorists, there was no lawbreaking. You had police officers up in a helicopter with sophisticated equipment, they got a little bored, they found a couple in a passionate embrace on a rooftop; they decided to follow that couple.

The second thing, though, that I think was telling about that we had a lot of discussion here about plain sight and the Fourth Amendment doctrines around – that what police officers can see in plain sight, they ought to be able to follow up on or to see, even by a camera. But just think about what you saw. What you saw was the use of extraordinary technology. You had a helicopter hovering above the city with camera equipment, the existence of which was unknown and unknowable to the people who were not simply on the ground in a public place, but on a rooftop in New York City. And those of you who know anything about rooftops in New York City know that people regard them as private places. They're dark. People engage in all sorts of behavior up on those rooftops. They don't expect that there's going to be a helicopter hovering above, with a camera; not only a camera, but with infrared technology that abused those police officers' -- what amounts to superhuman vision. The Superman's X-ray vision, in away. They can see in dark. And they don't expect to be seen that way. The extraordinary thing, really, about this footage is not only what it is -- it shows you about what happened, now almost 4 years ago -- but where we are now, in terms of video surveillance. One of the advantages of being among those last to speak here is that you can not only comment on what others have said, but, to some extent, you can look forward a little bit. I want to suggest to you that there have been three waves in the application of video surveillance in the Western world.

The first wave is that wave that, to some extent, we're still operating in, in the United States, and that's the sporadic use of mostly fixed cameras to surveil a limited number of places from a limited number of angles. It is sporadic. It's mostly what's been described here over the course of the last day or so. It's mostly what is in effect in the United States. The second wave really is in effect in some parts of the United States, and certainly in the United

Kingdom, which is well into the second wave. The second wave is pervasive video surveillance. If you've heard, they have 4 million-some-odd cameras, is the best estimate, in the U.K. I've heard the estimate that they spent 20 percent of their law enforcement dollars, or pounds, on video surveillance. It's pervasive -- other technologies are being used. It is networked. You have a combination of private/public surveillance which is occurring. It is something that we don't yet have, really, in the United States. There are a few places in the United States where there is more pervasive video surveillance, but we still don't have the U.K. style of complete video surveillance, if you will.

With the growing use of other technologies --you heard some of that be described here over the last day or so -- and this really, in a sense, is the third wave. The third wave is what, in New York City, is --the proposal is being introduced in New York City, and I believe this term comes from London. Perhaps Clive can correct me if I'm wrong. But the concept of "ring of steel." We, in the United States, have heard a lot about the ring of steel. The concept of "ring of steel" is 24/7 round-the-clock pervasive video surveillance, at least in particular areas of New York City, principally in the financial district in Lower Manhattan, but basically in Manhattan, more generally – pervasive video surveillance. It is combined with other technologies. The one that is most frequently mentioned is -- and we've heard some about this over the last couple of days -- is the use of automatic license-plate recognition technology that enables you to not only identify at least who is the owner of a car that is entering into a particular area, but to track that car as it moves throughout the day. There is some discussion of the use of face-recognition technology, so you can identify the particular individual who -- or individuals who are in that car. Face recognition, of course, is a notoriously imperfect technology, but that hasn't stopped the officials in New York from suggesting that they wish to use it. But, what you're talking about is the kind of complete round-the-clock pervasive surveillance that really typifies the surveillance society. And we are very close to that. Some parts of London talk about New York. There are suggestions, perhaps we do something like that in Chicago here.

I found it sort of interesting, actually, and I know this is not the doing of the Department of Homeland Security, which, I believe, asked. But the two most prominent municipalities in the United States, who have the most sophisticated video surveillance system, certainly the most sophisticated plans for video surveillance, were not represented here. That is, New York City and Chicago. I know a little bit about New York, and I know they don't like to talk about their plans in public. We've got FOIA requests in, trying to get a little better sense of those plans. But that's a shame that they weren't willing to come here and talk about this third wave, because that's where we're headed. It's not going to be the occasional town somewhere in Iowa or California or wherever, that has a limited number of video cameras trained in a small area; it's going to be this sort of pervasive surveillance.

So, what do we do about it? There has been a lot of talk here about best practices and voluntary codes of conduct. I am not a great believer in voluntary codes of conduct. I found a certain irony that so many in law enforcement and homeland security come in and talk about voluntary codes of conduct. We don't have voluntary codes of conduct for people who commit property crimes. We don't have voluntary codes of conduct for people who commit fraud. We certainly don't have voluntary codes of conduct, best practices for terrorists. We're not going to al Qaeda saying, "well, you really ought to institute a \best practices for how you go about doing your terrorism." We have laws. We have laws that, not only have consequences when you violate them, but we have an infrastructure for actually implementing those laws. That is what we need here.

We're talking about giving up some rights that I think are precious, that I believe many Americans believe are precious. When there are violations, not only the kind of bald violations that come with police officers, whether they're in a helicopter in New York City or in a control room in Florida, training their cameras on people of color or young attractive women, that there ought to be consequences for that. And so, the kinds of suggestions about laws that have been made here by the Constitution Project and others are important. I would add one element to that. I think there's got to be a private right of action. There has to be an ability for individuals who are harmed by the uses of these technologies and by these programs, to actually vindicate their rights, that sort of classic American approach to this.

We're frequently asked in this context who watches the watchers and whether or not we can put in sufficient safeguards to make sure that the watchers are well watched. But, in the end, there are going to be violations, not only the kind of bald violations that we're talking about this helicopter up above New York City, but violations of procedures and overzealous use. I'll close with this --let me give you an example. It's from a slightly different context. Some of you may know this example.

A number of years ago, the Detroit Free Press ran a series of articles about the use by law enforcement officials in Michigan of information that's in the NCIC -- essentially, the national crime computer -- extensive amount of information about individuals, much of which we now know is inaccurate. That's a separate problem, but extensive information about people. What they found was that people in law enforcement were using their access to that information for their own private purposes. We had one fellow who was checking up on an estranged wife. You had people settling scores. You had all sorts of what I would think people in this room would --who are to be good people-- say are outrageous uses of that, and also uses that waste -- you know, not are abuses of power, but waste valuable resources.

The remarkable thing that came out of that was not really a lot of denials by the police officials in Michigan that that had occurred, but that nothing occurred. Those police officers were not punished in any way, there were no consequences. We've got to have a system that creates consequences for that kind of behavior. One way in which to do that is to have a

private right of action. The people who were victimized by that should have had a right to go to court and say, "I was victimized. They abused power. I'm entitled to a recovery here. I'm entitled to some judgment against them." We need to have that in this context, as well. That's one of the things that has to be built into any legislation that's passed, is a private right of action.

MS. FRANKLIN: Before we have the next speaker, I just wanted to point that the Constitution Project does have a draft model private right of action as section 330 in the model legislation.

MR. McNEELY: Okay, thanks very much, Barry. Thanks very much, Sharon. The next person to speak, and the final person, is going to be Melissa Ngo, senior counsel and director of the Identification and Surveillance Project at the Electronic Privacy and Information Center. Before she starts, we're running a little bit late. Toby and I have discussed it, and we will continue with the question-and-answer after this, because we feel a lot of what these panels have said is very important. We're going to try to keep it a brief question-and-answer period, though, and would ask that you keep your questions brief, as well, when come up.

MS. NGO: Well, I am the last person to go, so a lot of what I'm going to say is going to be what has been said before. However, I will spare you the in-depth details and merely discuss them in terms of having it on the record. For one thing, to follow up on what Barry just said about the abuse of systems, it's not just that this egregious violation happened several years ago; just last year, the Department of Commerce came out and explained how one of their employees was able to use the TECS database -- it's a Treasury database filled with personal information -- in order to access it 60 or 70 times over the course of a couple of months to stalk and harass his ex-girlfriend and her family. The fact that this was capable of occurring in this day and age, with all that we have learned about the possibility for stalking and insider threats to privacy, it does bring up the very real question of how we make sure that there is accountability. And EPIC agrees with Barry that there does need to be a private right of action, because people will ensure that their rights are protected, because, otherwise, overloaded oversight commissions probably wouldn't be able to follow up on the violations.

So, let's start. Best practices involve the public and civil society from the beginning, clarify the purposes, set clear, objective standards, because that is the only the way the public can evaluate the effectiveness of a CCTV system. Employ data minimization. Data retention, collection, and distribution need to be limited to the minimum necessary. Need to establish strong legal safeguards, stringent reporting requirements, methods for public complaint, private right of action, and penalties for violations. We hear a lot about stalking, and we hear a lot about voyeurism, but we also need to ensure against racism and other forms of discrimination. We need to ensure that we do not squeeze the definition of "privacy" into ineffectiveness, and we need to visually guard against mission creep.

So, what am I talking about when I say "squeezing privacy?" Well, we've talked about it a little bit over the last couple of days. Though it seems counterintuitive to have privacy in a public space, this has to do a lot with how people perceive their interactions, like Clive was talking about. Memory is very different. The memory that a police officer or anyone walking down the street has of you is completely different from the memory that a camera has, where it can record and include, for infinite replay, zoom, scrutiny, your actions. This changes the environment. Increasingly, there is a shrinking of the public -- of the private space that people understand, and a shrinking of their idea of what privacy can be.

At EPIC – and we've testified about this -- we believe there is a right to privacy. Specifically, anonymity, even in public spaces. It's the freedom of not being identified. Should individuals be filmed entering addiction recovery clinics? Should individuals be filmed entering adoption clinics? It isn't merely addiction recovery program patients who value privacy, but all patients. The U.S. Department of Health and Human Services has said that privacy is necessary for the effective delivery of healthcare, both to individuals and to populations. Think about it. Imagine if your doctor visits were broadcast publicly. Would you still enter that fertility clinic? So, changes in technology should not eviscerate this right to privacy. This is why EPIC urges strongly against the creation of CCTV systems that allow continuous general surveillance of the public.

Mission creep. We need to guard strenuously against mission creep, because it makes CCTV a moving target. If camera surveillance is not effective for the goal of reducing violent crime, then let's use it for another one -- issuing tickets. The technology is converging. Barry talked about the "ring of steel" in New York. It's a $90-million plan partially funded through DHS grants, adding 3,000 cameras, license-plate technology, to track every single driver who enters and exits the area, and also, it's going to attach a fee to them entering and exiting the area. That would be how they'd be paying for this. New York is also considering the use of face-recognition technology in order to identify people --again, shrinking of private space -- where, in your car, people can instantly identify you when the technology gets better. Right now, the technology is not there yet.

One example I like to cite about the usefulness of face recognition technology is two individuals in an Australian airport decided that it would be fun to swap their passports, and the face-recognition technology system did not catch this. So, when we talk about the effectiveness of that identification system, know that it will get better, even though it's not quite there yet.

We need to talk about where the technology is going to now. There are talking cameras -- we've discussed this a little bit -- in the U.K. and in the U.S., where the watchers will be watching you, and then they will respond and give out orders. In the U.S., this has been happening in housing complexes, where private security guards have been yelling at tenants, saying things like, "get your fat ass off the corner," telling people that they're not allowed to

sit in front of their own stoops. I mean, loitering in front of your own home? Can you do that? Apparently, you can under these security guards' ideas of what you can and cannot do. There, we see the changing nature of it. It's no longer the police with their regulations, it's now the private security firms. And what are their regulations? What do they want to protect?

And then, we can talk about how Chicago is considering putting cameras with license-plate recognition technology on their street sweepers in order to be able to ticket people if they don't move their cars for snow removal. Further and further, we're getting away from what the public was told camera surveillance systems were originally to be used in order to sell them to the public, which is reducing crime. We need to talk about what the true cost of CCTV is. If we talk about money, Clive has told us there was 5 billion pounds spent in the U.K. over the last decade, 1 billion pounds of which were from public funds. DHS has spent $230 million in its grants through December 2006, and millions more are spent by cities and localities, and by residents who are taxed for driving into the middle of New York.

Then we have the questions about civil liberties, free speech, and the culture of accepting constant surveillance. We also have to think about -- again, back in monetary terms-- the fact that every dollar that you spend is being taken from a different, more proven effective security program.

Third, we need to consider the cost to safety, because for one thing, a February 2005 U.K. Home Office study discovered that one negative effect of cameras is that the vigilance of police and residents may decrease as they begin to rely on CCTV, creating both additional possibilities for crime and reducing the benefits of vigilance. This is a significant danger. We need the public to be aware. We need the public to be connected to their safety. One example is that this summer vigilant citizens, not the cameras, were the ones who alerted the police in London to the problems. They called in because they saw smoking cars and this is how things began. We need the public to be a part of their own safety.

There are a number of issues that must be thoroughly and openly discussed and resolved with public input before a camera surveillance system is installed, as everybody has discussed. And --obligatory plug -- if you want to learn more about the different kinds of myths of security under camera surveillance, my chapter and the book will be out in March. On our Website, epic.org, we have model legislation. We have more information about biometrics, face recognition, video surveillance cameras, all of that. Thank you.

MS. LEVIN: Thank you, Melissa. I want to provide an opportunity, if there's any questions from the audience for the panel. I appreciate your sticking with us through a longer morning than we had anticipated, but privacy is more important than your lunch.

[Laughter.]

MS. LEVIN: At least, I still think so. If there are any questions to the panelists, or any last comments, we definitely would like to hear from you. And we have Mike Fergus coming to the microphone. No cameras here, by the way. I asked the hotel, before we started the program, "Do you have cameras?" And they said, "No, we don't use cameras." So --Mike?

MR. FERGUS: Yes, I just wanted to follow upon Ms. King, earlier mentioning the IACP's work on the guidelines. That's the public-sector -- the Private Sector Liaison Committee, working with groups like the Security Industry Association, ASIS, and others. They are going to be working on that, and I'm hoping that the event that we have in February can follow up on these conversations and do that. It's really designed as an educational event for entities who are putting in surveillance systems.

The question I had, and I'm just wondering if the panel would address this--has there been any consideration of forming some sort of an accreditation board, maybe, working through CALEA or one of these other organizations, that could go out and -- with the input if everyone, design some criteria and actually allow the agencies, the cities, the municipalities, to voluntarily submit themselves for accreditation, to come down and have an inspection and perhaps say that this has been accredited by the CALEA Surveillance Board or the DHS or something like that?

MS. LEVIN: Anyone want to respond?

MR. NESTEL: I know that CALEA does have elements that address CCTV, but it certainly doesn't have a separate segment, and I think that's a great idea. But I also think a great idea would be if IACP came up with a model policy. I mean, you've got 1,000model policies, but none addressing CCTV, and I think that would be a good idea, too.

MR. FERGUS: Yeah, and the recommendation is going forward to the policy committee right now to do that.

MS. LEVIN: Well, I definitely think the more folks out in the private sector and in public sector that work on this issue and bring together their ideas on what are models, and then we can work with those together, I think, would be a great asset, and we look forward to working with you and your organization, as well. Thanks, Mike.

MR. STEINHARDT: Can I just add one thing to that, Toby? I don't recall whether you were then with the IACP -- but I actually spoke at that conference that took place in 1999, and I, at the time, described myself basically as the designated skunk in the room –I was the lone civil liberties representative. I went back last night and reread my talk, the text of my talk from back then, now almost 8 years ago, and what was remarkable were a couple of things. One, that -- at least, remarkable from my perspective -- one was that a lot of what I found myself talking about was the promise then, back in 1999, that there would be voluntary guidelines, and everyone would observe them, and all the horrors that -- some maybe of which have

come to pass -- would not, because those voluntary guidelines would be adopted. And, of course, none of that has happened.

Secondly, was, in a sense, how primitive the technology was in those days. It was a bunch of fixed cameras in a few locations. Even in the U.K. the technology was fairly primitive. We've gone so far beyond that, and we're so far beyond the point where some voluntary guidelines are going to solve the problem. We need some laws. I continue to be stunned at the notion that the law enforcement community finds laws to be anathema, that you would prefer to have voluntary guidelines to laws. Why -- if the rest of us are subject to law, why aren't you?

MS. LEVIN: I don't know that we had --speaking for law enforcement folks, I don't think we had any of them say that they would object to laws; I think the focus was -- they were always asked about, "what guidelines or what policies do you have in place?" But I don't think we heard any law enforcement representatives say they were opposed to laws. We always like to work on many tracks. If there are lawmakers here in the audience or that will learn of this workshop, and they're interested in making laws, obviously that's their prerogative, but –

MR. NESTEL: I don't think that law enforcement is opposed to the introduction of legislation, but every profession has voluntary codes of conduct, even the bar, and –

[Laughter.]

MR. NESTEL: -- and I think that often is the first step before you go to legislation. I think that police departments function with policies, and I think that that message has to get through first. And legislation can certainly follow.

MR. STEINHARDT: You know, if I could just respond to that, because this is an important point. I appreciate that the stated purpose of this was to talk about best practices, but I've been listening intently over much of the last 2 days, and certainly there has been, from the representatives of law enforcement here, and from the Department, at least the implication that laws are not necessary. But, beyond that, it is not true that we don't have laws in a number of other professions. I mean, if you take the legal profession, which I suppose I am a member of, what might have been voluntary codes of conduct 100 years ago are now enshrined into laws in all 50 States, and there are real consequences for violating those, not only those laws, but the ethical rules. At least a violation of the ethical rules results in your being drummed out of the profession. That's the kind of consequence that we need to have here. I'm happy to sit down with anybody in law enforcement who wants to sit down and seriously discuss the law, which we can introduce into Congress or any State legislature. But I made that suggestion back in 1999, I'm still waiting for somebody to take me up on it.

MR. McNEELY: I'd just like to comment, from the standpoint of the counsel for Civil Liberties Programs in the Department, not on the advisability of whether we should have legislation or not -- that's above my paygrade to suggest to the legislative bodies -- but just

that the issue of rule of law is one that concerns us, and we proceed with great caution when it comes to suggestions about how we should govern State and local law enforcement activities, how they go about doing their daily duties, to include critiquing their policies and the choices that they make in the exercise of their ministerial functions. We have the greatest solicitude for individual rights, but we're also conscious of that delicate balance between State and Federal power. So, if we have a tone of caution, if that's what you're hearing from us, then you're hearing the correct pitch. One of the reasons we are here is to listen and find out what our colleagues in the States and localities think they need, and then we go back and talk about inside the agency. When we confer with the legislative branch at the Federal level, we speak with them, and we let that inform our policies and programs. The privacy officer can speak to this.

MR. TEUFEL: I just want to make it clear --consistent with the Anti-Lobbying Act.

MR. McNEELY: Thank you. Okay, and, just so he gets the correct pitch, I'm not advising on the --whether or not legislation's good or bad.

MR. ZOUFAL: Just a quick comment. First of all, I -- with regard to the additional burdens that you put on the -- or suggestions of burdens to place on the grant process, I wouldn't. From a person who's worked with the grants, who's prepared the grant and grant applications, they're already quite cumbersome, as it is, so DHS should be mindful before any additional requirements are placed on the grant process.

And by way of question, I do think we have laws that govern this. I think it's the Constitution of the United States. I'm surprised that the ACLU would take a position that somebody whose Fourth Amendment rights are violated, or First Amendment rights are violated, would somehow not have a remedy, because that's not been my experience as general counsel at Chicago Police Department or my years in the corporation counsel's office, that there are, in fact, remedies. I'd be surprised if there wasn't a remedy for those individuals who were filmed on the top of the roof. I would think 42 U.S.C. Section 1983 would fit quite nicely. I guess the question is, why is that remedy inadequate?

MS. FRANKLIN: I'm not going to respond on your specifics about the people in the video, but I would say that, certainly, our position with the Constitution Project's guidelines is that this goes beyond what I think any court would find today in interpreting it. The legal panel that went before us talked about that in more detail, about the state of the law as it's developed right now and what actually might be required by the Fourth Amendment. But I think it's furtherance of a lot of those principles, the same kind of principles about what's protected by the Fourth Amendment and the First Amendment, and trying to enact that into law to set up those safeguards that would carry out those same principles, those same protections, balancing the needs here. But, I think, none of us would claim that what is in here would --or much of what's in here goes beyond what might be required by any court today.

MS. LEVIN: Deirdre?

MS. MULLIGAN: I have three questions. So, the first is to point out, I was actually surprised that no one mentioned the E-Government Act of2002? The law basically requires the government, to the extent the Federal government and Federal agencies, if they're going to deploy systems that affect personal information or the privacy interests of individuals, to go through this privacy impact assessment process. One of the things that I think's most problematic about the DHS model of deploying video surveillance systems is that it's occurring through grants to the States that completely circumvent congressional will that the privacy effects of technology be understood and explored and mitigated. And so, I actually think that there is, right now, a huge gaping hole through which we're driving millions of dollars in trucks to the States for surveillance cameras. I'd like people's thought. I can make a nice administrative-law argument that we should be able to convey that requirement downstream to the States through grant conditions, because I think there's a very strong expression of congressional will that technology be guided by privacy considerations. I'm kind of surprised none of the panelists made that argument right now. And so, I'm inviting you to make this argument.

And, two, I just want to suggest, operating in areas of legal ambiguity is often not very good for people who are making massive investments. When you're building a system, you want to know that you're not going to have to retrofit it because you guessed wrong. I'm wondering why law enforcement actually isn't designing their own guidelines of -- there's a push and a pull. I think it's very interesting, Mr. Nestel, when you looked, that 70 percent of people are operating in the absence of guidance. Police departments are not really naive about the fact they have big targets on themselves. They get sued a lot. And so, what it is it -- why aren't they developing practices? Because, in many ways, having best practices, particularly in the absence of law, is a great shield. I'm wondering, why is this happening? I'm hoping people will do question 1and then question 2.

MS. LEVIN: Well, let me start with the first question, on privacy impact assessments. The DHS Privacy Office did do a PIA on the SBInet use of cameras, and we actually benefited from a model PIA that Deirdre Mulligan and her graduate students at Berkeley had developed and shared with us. We have a standard PIA template, but it was very helpful to inform our PIA model with their work, because then we tailored it more specifically to CCTV. So, that was, I think, very helpful. We hope to use it going forward in other programs where DHS is the operator.

The issue of whether we can impose PIA requirements on grantees is something that we'll have to, obviously, take under consideration and discuss with various programs within the Department that work with our office. But we very much appreciate your recommendation.

MS. COPE: And if I can just respond. This, kind of, has been my thesis, and I haven't done a deep legal dive into whether or not it's actually going to work. I guess it got lost in the rush

of my presentation, but, I know that, for the big, huge homeland security grants, that there are already specific requirements that grantees have to make assurances that they're following certain Federal laws. I think the charge for the Privacy Office in DHS is to figure out if there are other Federal laws that they can make grantees follow, including the E-Government Act, and, perhaps, FISMA-type security issues that really drive at the heart of privacy and civil liberties? Right now, assurances that are required by the grantees relate to civil rights, which obviously is relevant to what Jim does, and that's important, but, you know, the assurance that you're not going to have conflicts of interest, that's random. If you can make a grantee promise to do that, then why can't you make them promise to not violate privacy rights and Fourth Amendment rights and First Amendment rights? So, I think, working with OMB and doing a real deep-dive legal analysis into what conditions and what requirements we put on grantees is really going to be the charge of DHS. And to, hopefully, also respect federalism.

MS. FRANKLIN: We would certainly agree that one thing that is going on here is that, with the availability of these DHS grants, it's skewing the cost-benefit analysis, to the extent that it's being done at all, by a number of municipalities just because if the money is available for the video surveillance. But you can't get that grant to go toward better lighting or cops or what have you. That that skews that process. Although we certainly would hope that communities would still try and go through that analysis, to the extent possible, and do that before applying for a grant.

And also, to echo the call, Jim mentioned there's a sensitivity to how much you impose on the States -- the grant recipients, but at least --and maybe at a general level, just a basic requirement of a privacy policy, of going through the process of a civil liberties impact assessment without dictating how that's going to come out or all the detailed provisions that would be contained in it. Maybe with some guidance on possibles, but not mandating it -- would be a strong step in the right direction.

MS. COPE: And can I just respond, real quickly, again also? I quickly mention this, play off of what Sharon just said. I'm not an expert in grant making law. I've done some research in it, but I'm, by no means, an expert. I think that there really is a problem. In terms of how those grants are structured -- if a local community notices or decides that there is a problem with a high-risk location, like San Francisco, where the Golden Gate Bridge really could be the target of a terrorist attack -- if it's local crime -- vandalism, graffiti, whatnot -- but there are these sort of protecting-the-homeland concerns that DHS cares about and localities care about, and then it's the issue of, what's the best way to address that problem? And if there are billions of dollars available to protect the homeland, but those dollars can't go to better lighting, to more cops on the street, or to different technologies, other than video technologies, that might be more privacy protective, I would guess, the charge would be -- to DHS -- to figure out if there is away to restructure those grants, because the idea is that we all

have a common goal, and there's this problem of how the money is funneled to reach that goal.

MR. NESTEL: Regarding the policy, I can only tell you, in Philadelphia there was tremendous debate about what department was going to be responsible for the camera system. The police department didn't want it. So, at one point, the police department even had me draft a policy for another operating department. And they didn't want to adopt it, because they didn't want it, either. So, that's Philadelphia's dilemma. I think, in other cities, I believe that their systems came quickly. I think that the money came quickly for them, faster than the policy. I also believe that, in their minds, it was a pilot program. In my mind, I think you still need a policy, even when you have a pilot program, but I've seen, in other jurisdictions, that during that pilot-program period, it's the growing pains of trying to figure out what the system can do, and what it can be used for.

MS. LEVIN: Tom, do I understand you correctly when you're saying that the law enforcement -- the police did not want it. They didn't want the system, or they didn't want to develop policies?

MR. NESTEL: The Philadelphia Police Department did not want a camera system. It was decided by the voters, and the city government determined that we would have CCTV.

MS. OZER: Toby, I just want to reiterate, on question one, that what we're seeing on the ground really is a result a lot of times DHS money comes down that doesn't have any kind of processor structure, and that is all flowing down to the local communities, who, their normal structure and process is being circumvented by the fact that homeland security money is available. In the '90s, when this money was coming from the general funds, when it was coming from the budget process, there was public process, there was public discussion, there was thorough analysis, and decisions were the best outcome of all of the community members and all the stakeholders. I think that it's a serious problem, both because of what Deirdre's mentioned about the Department DHS being charged with doing privacy impact assessments, and being charged with actually making strong and efficient policy for making our country safer -- that that money is going down, not with a lot of requirements, but with some kind of process and some kind of structure, so that communities are thinking through these issues, and not just thinking, "this is free money." Let me throw out something, because pilot programs -- what starts as, quote, "pilot programs," quickly expand. San Francisco was a pilot program 2 years ago with two cameras in one corner; it's now over 70 cameras, and is seeking DHS funding. So, I think that this is a serious probably. "Temporary" does not mean "pilot." If it's two cameras, even, that needs to be discussed and it needs to go through a public process. I think that it is the responsibility, if you're sending down these millions of dollars, that you send it down with a little bit of guidance, at a minimum.

MS. LEVIN: All right, I'm going to let Deirdre have the last comment, and then we'll have HugoTeufel, our Chief Privacy Officer, close.

MS. MULLIGAN: It is a comment. There's a difference between public process and expertise. And when we, for example, think about environmental planning, yes we involve the public, but we also have experts that provide information because we value their expertise. While DHS may be sending money down that's circumventing the public spending process, I wouldn't want to suggest, in any way, shape, or form, that that public process has embodied the level of expertise and sophistication necessary to evaluate the systems. I think one of the things that DHS can do is make sure that we get both process for the public, but also actual expert analysis of systems, and that we're not going to get that if you just say it has to go through the regular budgeting process, because there's not the kind or expertise that one needs. And I don't want to-- public process is great -- we need it; but the expertise of privacy and technology people who can evaluate these systems is invaluable. I just want to make sure that's on the record, that those are not substitutes -- they're not interchangeable pieces, they're integral.

MS. OZER: And that's why there's both recommendation one about things that DHS should do, and recommendation two, the kind of guidance that needs to go down to the States. I think that, within the public process, the opportunity to have a notice-and-comment period, as well, within those individual entities, so that there is the opportunity to give really informed information to those cities, so they're not just listening to a person on the corner who might not necessarily have all the information, and that that person on the corner actually is given the opportunity to make an informed decision.