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 LEGAL AND POLICY PERSPECTIVES

MS. LEVIN: Let me introduce you to our panelists this morning.

To my right is Chris Slobogin. Chris is a Steven C. O'Connell chair at the University of Florida, the Frederick G. -- I'm going to say "La'vinne" which is the way I pronounce it, but it probably is Levin -- okay, we'll mention it again -- Frederick G. Levin College of Law. And he's just published a book, which he happens to have -- please show the cover – Privacy at Risk: The New Government Surveillance and the Fourth Amendment. So, it was great timing for us to have him join this panel.

Next to Chris is Marc Blitz. Marc teaches constitutional law, national security law, and related subjects at the Oklahoma City University School of Law, and he, too, has written a number of articles regarding CCTV; a list of them, or a partial list, is in the bios, which you have in your packet.

Directly to my right is Fred Cate, who's the distinguished professor of law and director at the Center for Applied Cybersecurity Research at Indiana University and a senior policy advisor with the Center for Information Policy Leadership at Hunton & Williams. He's also written a number of articles and books on privacy.

Deirdre Mulligan, to my left, is the director of the Samuelson Law, Technology, and Public Policy Clinic, and a clinical professor of law at the UC Berkeley School of Law. Deirdre has been working on privacy issues for decades.

[Laughter.]

MS. LEVIN: I first –

MS. MULLIGAN: Almost as long as Toby.

MS. LEVIN: My very first workshop at the Federal Trade Commission included Deirdre. So, we go way back. And then, Jay Carafano, who is with the Heritage Foundation. He is the assistant director of the Katherine Shelby Cullom Davis Institute for International Studies at the Heritage Foundation, and is a leading expert in defense affairs, military operations and strategy, and homeland security, and is very well known -- is very knowledgeable about activities at the Department of Homeland Security. So, with that introduction, we've asked Chris to set the stage for this panel and give us some background on exactly what is the current state of law in this area. And we'll begin with that. Chris?

MR. SLOBOGIN: Okay, thanks, Toby. I'm going to focus primarily on the Fourth Amendment, which I think is the most important constitutional provision relevant to regulation of surveillance, and specifically, closed-circuit television, what we're calling CCTV. Those of you who know the Fourth Amendment know that what you see on this slide is not the precise language of the Fourth Amendment. But what the Fourth Amendment says in effect, is, "People shall be secure from unreasonable searches and seizures of their houses, persons, papers, and effects."

So, the Fourth Amendment is not implicated unless the government engages in a search or a seizure. There has to be government action that results in a search or a seizure. So, it's very important to define what the word "search" means.

Now, a layperson, of course, could define "search" in terms of looking for something or examining something. If that were the definition of search for Fourth Amendment purposes, CCTV would be a search, because cameras are used to look at, or examine, what's going on in public and private spaces. But that's not the definition of "search" the United States Supreme Court has adopted. Instead, what the United States Supreme Court has said in the case of Katz v. United States, is that a "search" is a government action that infringes expectations of privacy that society is prepared to recognize as reasonable. This is called the "reasonable expectation of privacy" test. I'm sure virtually all of you have heard about this.

So, the 64-million-dollar question (the actual amount of money depends on how much DHS is willing to shell out for all of this)–

[Laughter.]

MR. SLOBOGIN: -- the big question is, what is a "reasonable expectation of privacy" in this context?

Well, clearly, we expect privacy in our homes. If the police physically invade our home, that is going to be a Fourth Amendment search. But what if the government doesn't barge into one's home; instead, it looks into the home using either the naked eye or some kind of technology? I want to focus on this scenario first even though CCTV, as we've been talking about the last day, has to do with surveillance of public spaces. In the case of Kyllo v. the United States, decided back in 2001, the Supreme Court dealt with the use of a thermal imaging device to discern heat differentials inside the home from a lawful vantage point outside the home. The Court said this was a Fourth Amendment search. So far, so good. But in the course of saying that, Kyllo also said that looking into a home may not be a search if the police use the naked eye or if the police use technology to merely duplicate what a cop standing on the sidewalk could see with the naked eye. In other words, if a thermal imaging device is used to discern what could be seen by the naked eye through a picture window, that would not be a search. Further, even if the technology can see more than the naked eye -- goes beyond what a naked-eye viewing could discern -- if the technology used is what the Court called "in general public use," then, once again, we don't have a search.

Now, a thermal imaging device is not in general public use. Such device, the Court said, is not something that members of the general public can get their hands on easily. But binoculars, flashlights -- conceivably, that is technology that is in general public use.

So, what does all this mean for CCTV? Well, one could argue that using a CCTV system, to look inside the home is not a Fourth Amendment search. Why? Because it only duplicates what a cop could see with the naked eye from the sidewalk. Now, I think there are distinctions. If the camera system is up 24/7, has zoom capacity, night-vision capacity, and all the other gadgets and gizmos that we've talked about, that is going beyond what the cop could see with the naked eye. And, also, you could argue that, since CCTV cameras are usually on telephone poles or on top of roofs, they're not really viewing the home from a lawful vantage point. In fact, a number of lower courts have said that, even if it's technically lawful for a cop to be on a rooftop or perched on top of a telephone pole, it's not normal; and, therefore, that would be a search situation. But I want to raise the possibility that, under the Court's jurisprudence in Kyllo, CCTV viewing of the home, of the inside of the home, might not be a search.

In fact you could argue further that cameras are in general public use, that they are technology that's generally accessible to the public.

There is a case called the Dow Chemical v. EPA, decided a couple of decades ago, where the Court made the astonishing pronouncement that a $22,000 mapmaking camera is in general public use, is generally available to the public. If that kind of technology is considered to be available to the public, if that's a technology that's in general public use, then, conceivably,

the cameras used with CCTV are in general public use. Now, Dow Chemical involved surveillance of curtilage, as opposed to the interior of a home; but nonetheless it might provide precedent for justifying suspicionless use of CCTV to spy inside the home.

Lower courts dealing with this issue have split on the issue of whether using binoculars, cameras with zoom capacity, night-scopes, and so on, to look inside the home is or is not a search. But, as far as the Supreme Court is concerned, the bottom-line answer to the question of whether you have reasonable expectation of privacy in the home, vis-a-vis CCTV surveillance, is, we don't know. All of the things you see on this slide right now were dictum. That is, the statements in Kyllo that summarize what you have here on the slide are statements that were not necessary to the decision, so we do not know for sure what the Supreme Court thinks about these issues.

Now, going to the issue of CCTV surveillance of public spaces, which is what we've been focusing on, the key case here is United States v. Knotts, decided in 1983. This case involved use of a beeper to track a car traveling the public thoroughfares. The Court said this use of technological enhancement devices was not a search -- that we cannot expect privacy in public, even if the police are using enhanced technology, to view what's going on in public.

However, the Court did reserve the question of whether what it called "dragnet surveillance," dragnet police investigative techniques, is a search, so it might answer differently when it is eventually confronted with that question. Knotts had argued that use of beepers to track someone, day in and day out, for days at a time, should be considered a search. And the Court said that since the beeper in this case was only used for an hour, it was not going to have to confront that question, but it suggested that if the beeper had been used for a much longer period of time, then a Fourth Amendment search might have occurred, even though only public activity was surveilled.

One other point I want to make with respect to what we talked about yesterday. Sometimes CCTV involves audio surveillance, as well as visual surveillance. Even if visual public surveillance is not a search, and it is very possible for the police to engage in a search if they conduct audio surveillance of conversations in public. In fact, the leading case in this area, Katz versus United States, involved bugging a public phone booth, which the Court said was a search. So, CCTV that involves audio surveillance could easily be a Fourth Amendment search.

The bottom line with respect to use of CCTV in public is that it's conceivable it could be a search if it involves 24/7 surveillance --what might be called dragnet kinds of surveillance--or if it involves audio surveillance. And, in fact, some lower courts have suggested, in dictum, that CCTV could be a search, under the right set of circumstances. I want to read to you from a footnote that happens to be in my book -- shameless plug number two –

[Laughter.]

MR. SLOBOGIN: -- the Costin case which says it may be a search "where video surveillance is aimed indiscriminately at public places and captures lawful activities of many citizens in the hope that it will deter crime or capture what crime might occur." Okay? Now, that is dictum, but, nonetheless, it is a statement by a court.

I also want to emphasize that if use of CCTV is a search, this conclusion would apply not only to government use of CCTV, but also to private use of CCTV that the government is taking advantage of. That is, if the government contracts with a private agency-- as it apparently does in Clovis with its contracts with Walmart -- or uses a private camera system in a one-way feed to the police department, that would also be governed by the Fourth Amendment, because the Court has made very clear that when the police use private agents or entities then the Fourth Amendment is implicated.

Okay, so, what if CCTV is a search? What if the Fourth Amendment does apply? Well, the traditional requirements, as most of you know, are that when a Fourth Amendment search is taking place, the police need to get a warrant based on probable cause, a fairly tough requirement to meet. However, the Court has also said that, if the search is not particularly intrusive, then perhaps a warrant is not necessary, and perhaps probable cause is not necessary. I think the most relevant cases, for our purposes are a whole series of Supreme Court decisions in the roadblock area, cases involving police using roadblocks to stop individuals on the roads.

The key case here is Indianapolis v. Edmond, though there are least four other Supreme Court decisions that deal with roadblocks. And what the Court has said in these cases is that it's permissible to conduct a roadblock without a warrant and without probable cause, so long as a higher authority authorizes the roadblock -- in other words, someone other than a field officer authorizes the roadblock -- and either the police who are implementing the roadblock have reasonable suspicion (a lower level of certainty than probable cause) to believe the person they're stopping has evidence of crime in their vehicle or has committed a crime, or there is proof of a significant crime problem that the roadblock is designed to address. For instance, the Court has upheld sobriety checkpoints on the theory that we have a serious drunk-driving problem, and so, it's permissible to use roadblocks in the absence of warrants and probable cause. Another case involved roadblocks to stop illegal immigrants near the border. That was another situation where the Court said roadblocks are permissible without a warrant, without probable cause, and without individualized suspicion of any sort, because of the significant crime problem it was designed to address. These roadblock cases could conceivably be a template for dealing with CCTV, something I'm going to come back to later.

Finally, I want to talk about other possible sources of regulation. I've focused on the Fourth Amendment. I think that's the most important source of regulation, but there are other possible sources of regulation. The first is the First Amendment. The question here is, Does

CCTV-- especially CCTV in public spaces -- does it chill freedom of speech, does it chill freedom of association? If the answer to that question is yes, the Court's case suggests the government needs justification in order to engage in use of cameras in public spaces.

Another possibly relevant constitutional provision is the Due Process Clause, from which the Court has derived the right to travel and, conversely, the right to repose. The question here is, Does use of CCTV in any way chill or infringe the right to travel or the right to loiter, so to speak? And if you can make the argument that it does, then, again, the government needs justification, under the Due Process clause, to engage in CCTV.

Also mentioned yesterday was the Equal Protection Clause. The question here is, is CCTV being used to intentionally discriminate against suspect classes on the basis of race or gender? If the answer to that question is yes, then, once again, there are conceivably constitutional implications.

And then, of course, there is what we spent most of our time on yesterday, legislation and municipal policies designed to regulate CCTV. As we heard yesterday, many jurisdictions do have these kinds of regulations, but we also heard that 70 percent of the jurisdictions with CCTV do not have a policy. And, even those jurisdictions with policies usually do not impose any sanctions for their violation -- a very important issue we didn't talk about. For instance, the IACP police that was mentioned, developed in 1999 and 2000, is a voluntary set of guidelines. What does that mean? There is no external auditing, there is no sanction imposed by any external entity if the rules are violated. Similarly, we heard, from Mr. Myers when talking about the Park Police rules, that he did not know of any sanctions ever imposed on anybody in connection with those rules. I talked to Chief Keyes yesterday in connection with the Clovis policy, and again no one's ever been sanctioned under those rules. Under the Fourth Amendment, you've got damages, you've got injunctions, and you've got the possibility of exclusion of evidence. So there is a significant difference, arguably, between constitutional regulation and the kind of regulation we talked about yesterday.

There are two last sources of regulation. I've been focusing on the Federal Constitution. A number of state courts have indicated that their state constitutions are more protective than the Federal Constitution. And there are even a couple of States that have specifically said, in dictum, that even though the Fourth Amendment in the United States Constitution may not regulate CCTV, the search-and-seizure provisions in their State constitution might provide a source of regulation for CCTV. This is something to watch for. There could be independent regulation of CCTV, constitutional regulation, based on State constitutions.

And finally, the last source of regulation could be money. As we heard yesterday, over and over again, given the unclear effectiveness of CCTV and the significant cost of CCTV, if the Federal Government weren't providing all this money, we might have, as a practical matter, very serious regulation, perhaps even the abolition of CCTV, because it costs so much and its effectiveness is not demonstrated. At the least, building on the suggestion made yesterday,

funding could be conditioned on the development of policies of the type that we're talking about. So, that's an overview of current law in this area.

MS. LEVIN: Thanks, Chris. I know it's a challenge to condense a lot of this into a very short summary, but I think you did a terrific job. I don't know if there's anyone else on the panel who'd like to comment on the summary -- feel free – or anything to add. Marc, go ahead.

MR. BLITZ: The one observation I would add is that the courts -- the Federal courts have made clear that use of CCTV in private environments -- by which I mean not the sorts of things that Chris was talking about when he was talking about the implications of the Kyllo case, but cases where law enforcement authorities have set up cameras inside of a home or business -- have made clear that that kind of video surveillance is subject to the Fourth Amendment, is a Fourth Amendment search, and is subject to requirements that parallel those in the Wiretap Act. So, for example, a Seventh Circuit case in 1984 held that in order for the police to use video surveillance in a private environment, they had to show -- they had to satisfy four requirements -- they had to show that normal methods of law enforcement -- alternatives to video surveillance -- have failed or are not worth trying; they have to, particularly, describe the nonverbal conduct to be surveilled and limit the period of interception to no longer than is necessary, and minimize the interception of conduct.

And other circuits have followed the Seventh Circuit. Most circuits agree and impose identical, or nearly identical, requirements on private video surveillance.

And one implication this has, I think, for public video surveillance is that, in these cases --one interesting feature of these cases is that, in figuring out what constitutional requirements apply to private video surveillance, the courts look, not just to other court opinions, but to statutes. They look to Congress's interpretation of the Fourth Amendment. And so, it's possible that the same sort of pattern might occur as the law of public video surveillance evolves.

That's all I have to add.

MS. LEVIN: Deirdre?

MS. MULLIGAN: I think -- while the Fourth Amendment is the focus that most people, kind of, go directly to, in the context of thinking about video surveillance and law -- I think it was really appropriate that Dan Sutherland, when he began our day yesterday, opened with a quote from Hamilton, basically talking about the risk of enumerating rights, and that, by enumerating them, we might actually cloud the policies and the principles that were animating those rights. And if you think about the structural constraints of the Constitution more broadly, the entire goal was to basically limit States' abilities to spy, control -- one of my professors in law school talked about limits on democracy and coercion, structuring the relationship between States and citizens. Sometimes when we focus too narrowly on whether or not you have privacy in a public place, we lose sight of the richer conversation

about, to what extent should the State be using resources in certain ways to spy on the general public? And I think that, in part, Dan's reframing, saying, let's step back and think about what was animating our decision to articulate the Fourth Amendment -- concerns about generalized searches, concerns about warrantless searches, concerns about unchecked police discretion. When we think about video surveillance in that way, we think about watching the many instead of watching the few, we think about technology that makes police activity completely invisible. All of a sudden, we don't know where the police are. And so, I think it's really worth stepping back. I think it makes sense to think about reasonable expectation of privacy, in part because we can think about the way in which video surveillance technology makes it completely impossible for one to assess what your reasonable expectation might be.

So, think about being in a public park and knowing that there are some really powerful cameras --and we had some installed on the Berkeley campus -- and with a camera which I could use, I could read the text message you were putting into your phone. Okay? That's how good they were. And I could do that from Estonia, because I could remotely control this camera. And I could zoom in and follow you. And so, all of a sudden, the physical boundaries of the space become completely indeterminate. You think you're in Berkeley-- and, in fact, you're in Estonia, in Russia, and, somebody's bedroom in New York, right? So, it's completely impossible to figure out the physical confines of the space you're in.

And then, think about -- typically, when we think about the police not having to avert their eyes, there's also this mutuality. I see you, you see me; I realize that the police officer is standing close to me, or standing in the same physical space. And the technology basically makes the watchers disappear. So, I have no ability to gauge my behavior. As a faculty member, I tend to behave slightly differently when I'm in a room full of my students than I do in a room full of my friends. Most of us tend to behave slightly differently -- not because we have anything to hide -- it's all about the social face we put on.

The temporal boundaries are completely eroded. When I think about, yes, I was in a public space; it's an ephemeral activity. I walked through the space. I didn't leave little tracks across the ground that emanated some version of myself after I walked through. I disappeared. You might have been there and caught me in that public place, but there's no permanent record about me being in that place. And now there is. And maybe it only lasts for72 hours, and maybe it lasts for 6 months when it happens to be on the Mall.

And these discreet events -- I thought it was very, very important that Clive started to focus this on the distinction between capturing images and recording images. And a little recording means a lot, right? All of a sudden, these discreet views of an individual life become this composite picture.

The Reporters Committee, which is a case that wasn't mentioned, looked at public records, and said, you know, yes, there are police files all over the place, but if we pull them all

together, there's something qualitatively different about this virtual current biography of everything you've done wrong or everything you've done right, or perhaps just everything you've done.

And so, if you think about a reasonable expectation of privacy, what exactly is left to inform it? I don't know where I am, I don't know who's there with me, I don't know how long I'm going to be here, and I don't actually know what you know, because I think you might know just what I'm doing today, and it turns out you've been watching me for 6 months. And it's really hard to think about what a "reasonable expectation of privacy" test looks like, I think, in that context.

And so, it's relatively important that you think specifically about how the technology alters our experiences of space, and then to think that these are not fungible places, which is something somebody brought up yes; these are expressive places -- right? -- they're the places that we have held for time immemorial as important to the public, as places for expression, demonstrations. And so, I think it's really important to think specifically about the changes that technology brings.

MS. LEVIN: Okay. Have the communities in the U.S. had time to consider whether or not the technology impacts this expectation of privacy? We heard, yesterday, from at least one community -- and I heard this from --actually, from several that I spoke to when I first approached them about this workshop, about CCTV, and they described the process they had gone through; they all said, "we spoke with our general counsels," and their counsels said, "there's no expectation of privacy in public space," period, done, that was the extent of the homework, that was the extent of the analysis.

To what extent have we, as a society, as a --as agencies, government agencies, considered the impact of the technology on this expectation? Or have we just simply decided the Knotts case and the Katz case control, and that's the end of the story?

MR. SLOBOGIN: Well, I tried to suggest that a cut-and-dried answer, such as we heard described yesterday, is wrong. The Knotts case is certainly precedent that could be used by the government to assert that CCTV in public is not a search, but Knotts itself has that dictum in which it mentioned that dragnet surveillance could be a Fourth Amendment search, and I think you can describe CCTV as a form of dragnet search. I think Deirdre very eloquently described how it can become dragnet, in terms of its effect on people. I think all the members of the panel have their own "horror stories," to use the language that others used yesterday, that might convince people that CCTV has more of an effect than one might think.

For instance, thinking along the lines of Deirdre was suggesting, imagine you're on a public street, and there is a camera on a telephone pole. Now, maybe 90 percent of the time, 95 percent of the time, you're not going to give it much of a thought, you're just going to walk along your way. I've been in London, and, I have to admit, I don't usually think about the

fact there's a camera trained on me every second that I'm on the sidewalk. But, let's say now you want to run down the street, or you want to obscure your face, or you just want to hang out on a sidewalk for a while, or you want to go visit your psychiatrist, or go to an Alcoholics Anonymous meeting, or see a lover. There are all sorts of innocent activities that can be significantly chilled by the kind of continuous observation that CCTV involves.

Now, this is subtle stuff, and ranged against 9/11 a lot of people pooh-pooh it, but on an everyday base it can have a significant effect on the way people behave, the way they think about themselves. Philosophers talk about the concept of double vision, that when you're being watched as you do something, you change the way you act, you don't act the way you normally act, because you know you're being watched. Cameras are a 24/7 observation of what you're doing. It can subtly and not-so-subtly change the way you behave. And I think that's what Deirdre's getting at, in terms of talking about what CCTV does to us as a society. It can affect the entire ambience of society, because of its constant surveillance.

MS. LEVIN: But have we seen any litigation? Cameras are not new. The communities are requesting them. We heard that yesterday from a number of speakers. So, is there really that -- a legal basis for objecting? Have we any kind of recent cases or efforts?

MS. MULLIGAN: Well, I mean, I think the courts have hinted, in several different cases, that if the technology got to the point where it was really pervasive, that there may be issues there. But in many ways, I think that the case law, because of the way in which case law develops -- it's incremental, it only deals with the facts before it -- are really not our best tool in thinking and formation of policy, because this is about, not what the law allows, necessarily, but what kind of society we want to occupy. And if we don't think about privacy in public place -- because I think privacy is a really difficult organizing principle; it hasn't been all that effective as a legislative tool -- and it also -- for many people, it doesn't really resonate strongly. You say, "well, you should be really concerned about your privacy," and they're like, "I'm in the middle of a park, what do you mean?" Right? Conceptually. But I think when you begin to think about criminal procedure and what animates it, and things like limiting discretion through judicial oversight, and we think about transparency, and we think about concerns about bias and systems of domination -- right? -- those are all things that criminal procedure has taken as things that, not we care about because we care about privacy, but we care about because we want policing to be appropriate, responsible, consistent with community ideals, other than just law enforcement, but also, you know, respect for individuals and respect for differences. And I think those things can help us think about what kind of constraints we might have on video surveillance. And, you know, the way in -- as I-- I mentioned it undermines transparency. I think, potentially, it leads to an enormous increase in unchecked discretion.

All of us would notice if we had a police officer following us around. Right? I don't know if you've ever -- I've been followed, actually. I've organized demonstrations and things, so I've

had, kind of, regular interactions with police. And you notice – I mean, even the ones that are really good, you tend to notice. And, certainly, if they weren't trying to hide themselves. But we've all been in places with cameras that have a sign that says there's a camera here, and very few of us actually take stock of the fact that, hey, that camera could actually be following me around. Right? And so you don't understand what it means when there's a camera there. You do understand when there's a police officer following you. But, in many, you know, instances, those could be exactly the same thing.

I think the fact that video surveillance focuses on visual images -- in many ways, it heightens our reliance on things like race and age, gender, which are exactly the kinds of things that we've tried to cutout of policing decisions. Because they're visual images, they focus us on those things that are visual. And there are other technologies -- people have talked about other kinds of sensing technologies that actually could help weed out some of those things that allow us to introduce bias.

I think that the technology also masks a lot of choices that -- you know, when people hear it's video surveillance, they think, "oh, it's somehow or other neutral," right? There's this neutral idiom of technology, oh, experts have to decide whether or not it's good, but we all know that technology engenders all different kinds of value decisions -- right? For example lots of false positives, lots of false negatives, who are we watching, who are we not watching? And the video surveillance, in particular, I think, can mask a whole bunch of decisions that probably warrant community participation. We heard a lot about that yesterday from the community panel. You know, people are like, yeah, we want cameras, and they don't really care about the research. And I think that there's an obligation to make people care about the research. People want a lot of things that don't work. Right? If you're spending public money, one would think that, giving the people what they want, if what it is is, as Bruce Schneider calls it, security theater -- perhaps that not really what the public dollars are supposed to buy. Maybe we should actually do a better job. There's this thing called education. We should teach people what the limits are of the technology. And part of that means making the technology something they can comprehend-- not just cameras, but cameras that have a whole bunch of different kinds of stuff that go with them.

MS. LEVIN: Okay. Jim?

MR. CARAFANO: Yes, I actually want to agree with you. I mean, I think it's a dual problem here. You've got two forces which are really unchecked. And she mentioned both of them. On the one hand, which you discussed yesterday, there is this -- the "do something." And then there's -- and with all the press coverage about London, everything -- there is this notion that this is something we can do. And the other is "spend money," right? And with the vast amount of Federal money out there, this is something we can spend money on.

Well, those are really unchecked forces, because those seem very natural compulses, and there are not very convincing arguments not to do that. And the other really unchecked force

is, "This is a great threat." And I think that you -- I think the panel -- even if you take the strictest interpretations of how you should apply the First and Fourth Amendment to these technologies, there's still an enormous space to employ these technologies, and they can still be incredibly invasive. And so, the law doesn't really help you, either.

So, neither one of these impulses are really unchecked, and neither one, I think, are really going to resolve the issue. And my theory is what's really required here is that if we adopted a utilitarian approach, we wouldn't have a problem. In other words, we would walk ourselves back from pushing the boundaries of a surveillance society, and we would address the issues of very inefficient and illogical uses of our -- of our funds.

You know, I think it's interesting, although the data is not persuasive, I don't think, on CCTVs as getting a lot of bang for the buck, and, at best, ambivalent, I mean, there is a lot of research data that says that in the last 20, 30 years community policing and problem-oriented policing are more effective than reactive policing, that proactive policing is more effective than reactive policing. And when you look at the strategies for employing these cameras, and which there usually is not, at best they're usually reactive. And, I mean, so that should tell you, there, that it's not necessarily going to be part of the most effective policing strategy you could get.

And so, where are the three big voids? If we had better risk-assessment methodologies which determine where the best utility is for different forms of policing programs, and takes into -- the cost factors and the impact on privacy and everything else -- if we had better operational research capabilities inside police departments to do this kind of analysis-- and if we had police departments and law enforcement agencies below the Federal level that actually did scientific research themselves -- I mean, primarily, most of the scientific research that's done is done by academia, and law enforcement uses that, but the law enforcement doesn't actually participate in that. You don't see very many law enforcement scientists. If we actually had these things operating in our communities, you know, my guess is we wouldn't see the expansive proliferation and demand for these systems that we're seeing, because people would just recognize that while there is some utility for these systems, it's relatively limited, and that would pull us back from having to really face the issues of living in a surveillance society or not. So, to me, I think, it's the expertise --it goes back to the expertise and the knowledge of the law enforcement communities themselves when they're adapting and going – speaking to their legislators and trying to adapt these programs, that really is the most significant issue in going forward in these kind of systems in a logical, rational, and good public-policy manner.

MR. CATE: Yes, I would like to very strongly echo what James has said. And I think it also moves us in a direction that is, in fact, in some ways, most useful for this discussion, which is, at the end of the day, the great determiner here is not going to be a Supreme Court decision. If we're waiting for a court to say, "this is unconstitutional," or, "it's constitution," or

whatever, we could we be waiting decades, and I doubt if we're going to find anything very useful.

I would remind you, an enormous number of potentially promising programs for fighting crime and fighting terrorism have gone down in flames, without any involvement from courts whatsoever, because the public wouldn't put up with them, because Congress wouldn't put up with them, because they cost too much money and didn't deliver sufficient results, or because they raise such administrative burdens to run them that they eventually collapsed. Homeland Security has certainly had its experience with those; and I'm sure many other local and State authorities have, as well.

So, I think, in some ways, what we really need to focus on, in some level, is the more practical side of the legal question, which is, what do these things cost, what effectiveness do they deliver, and how does that relate to the promises made for them?

And, frankly, it's one of the great ironies of this--that video systems in the U.S. have been largely sold on the basis of -- they would fight terrorism, they would secure the homeland. In fact, the one thing the research seems very consistent on is that they have no effect there. It is a completely wasted effort to think you're going go fight terrorists by putting cameras up. You may catch them after they've committed their horrendous terrorist act, but that, presumably, is not what we mean by "securing the homeland." We don't mean getting convictions after they've blown themselves up on the airplane. We need a better system to fight terrorism, and cameras aren't it. They just don't work, so far, in that area. They work in other areas. There are other uses, which we heard yesterday, demonstrated clearly, although, again, I would point out, selectively. Every time you see a video clip, where you say, "here we captured somebody doing something wrong," remember the 6 million minutes of video you're not seeing, where you captured people doing nothing but living their ordinary lives and exercising their constitutionally-protected freedoms.

So, again, we're talking about an extremely ineffective technology for what it's being sold for. Remember, though, it has costs beyond just money. And you might think practically about what some of those costs are. They're almost all legal in origin, so I think they appropriately apply to this panel. For example, what happens when you get requests under your State Freedom of Information Act for those records? Are they exempt? Has your State legislature exempted them? If not, who's going to have the joy of watching them to find the segments that respond to those requests? This is not hypothetical. We deal with this every single day with e-mail, right? We get e-mail by the billions. We then get requests for those e-mails. We have to supply, we have to respond.

State laws are often much more disclosure-oriented even than Federal law, so don't think, because there are Federal rules that might be of help here; although, frankly, I can't think of any in this specific instance; what you have to worry about are the State laws that you're going to be dealing with. Right? How much time are you going to spend providing this --

how much time are you going to spend responding to subpoenas for the data for other uses? Alright? This is one thing we've learned with the toll pass, the EZ Pass system, and so forth; litigators rapidly discovered these were very useful records for determining where was the spouse going when he was supposed to be going to work but was actually out with his little floozy, or whatever. So, we subpoena these records, and then the entities that hold them -- in your case, police departments -- have to spend their time responding to those subpoenas. Right? Is this what you want to do?

I was, frankly, shocked yesterday -- I was stunned into silence when one of the people on the law enforcement panel said, "we didn't really know how the people in the dispatch room were going to react to this, so we just put it in there and though we'd see what they did with it." Is that the way you build a secure technology? Right? We're just going to put this -- that's going to capture images, and then see how they react to it. These are the types of costs. Right? Is that what you want to be explaining in the newspaper?

Today's USA Today, slipped under my door, says, "Police Brutality Cases Up 25 Percent, Union Cites Lack of Resources for Training." So, now the story is, we took the money we could have put into training police officers, who we desperately need on our streets, and we put them into cameras instead. Right? That's a cost. That's money that was spent in one place, could have been spent in another. Those are the types of issues I think we should be, in many ways, most concerned about. And I would just, finally, note, the point was made yesterday that this is really all about perceptions. Doesn't matter if it works or not, it's: what do people think? And, in fact, there's a lot of truth to that. That's why a lot of, particularly, private businesses, put up fake video cameras. Maybe it's a recommendation for the government. They're cheaper, they don't pose any privacy interests whatsoever, and if there's a deterrent effect of having the little flashing light in the camera up there, maybe that would accomplish that. But, remember, perceptions work the other way, as well. Why didn't you catch that guy if there were 30 cameras on him when it happened? Why didn't you protect this person? Why wasn't that camera working? We've seen extensive litigation, where people have put in emergency-call phones, or they put in lights to protect, you know, dark paths in university campuses and cities; those go out, they don't work, somebody's attacked, they go for the emergency phone, and it doesn't work. Now you've bought yourself a lawsuit. Has nothing to do with privacy or the Fourth Amendment, but it's just a classic old lawsuit. This is the type of issue which would keep me up nights if I were rolling out these systems without having done the type of analysis that James was talking about.

MS. LEVIN: Yes, Marc?

MR. BLITZ: Just one brief follow up to what Fred said. Yesterday, if I'm recalling correctly, Commissioner Jones said that people's perceptions about video surveillance changed and became, I wouldn't say-- if I'm remembering correctly, they didn't reject the use of video surveillance, but at least raised concerns when they thought more deeply about the kinds of

things that might happen when you have a permanent video surveillance system in place. So, I think that, even though perception -- public perception is very important, it's also important to have thorough conversations about what's likely to happen, because, if you don't have that, people are likely not to think too carefully about what video surveillance will mean for them -- for their privacy, for their liberty, for other things they care about -- and the kinds of things that Fred was just talking about. For example, the things that have happened in the wake of installation of intelligent highway systems, like EZ Pass or request-- or FOIA requests, are probably things like this, things that citizens don't think of at all when they're thinking about what public video surveillance will mean. So, I think what's important is not just public perception, but educated public perception, by which I don't mean a paternalistic formation of that perception, where researchers or academics tell people what to think, but, rather, a thorough conversation where people decide for themselves what they think of video surveillance, but do so after very carefully considering what's likely to happen when those video surveillance systems go up.

MR. CARAFANO: I want to make one quick follow up on the forensic thing, which I think is normally the most commonly used and strongest argument is: "well, we have a picture of them doing this." In fact, you get the same arguments for screening all the containers that come in the country that, after the nuclear weapon goes off, we'll be able to tell you which container it was in.

What I would -- and I haven't seen this; maybe somebody else on the panel has -- what I haven't seen is, and I would really like to see, is some more serious research about, okay, that is a benefit, okay, but there's no cost-benefit analysis. There's -- what are the other ways -- what are the other forensic means I could have used to obtain that data? You know, we got some video surveillance, I guess, from the guys in the Oklahoma City bombing, because they used the ATM machine. But, I mean, the key forensic data was the VIN number off the vehicle. They could have gotten that same VIN number off the vehicle in London and achieved the same thing. And so, I'd really like to see some analysis of, well, okay, yeah, this is one way to get forensic data on particular terrorist acts in which there's the least good data, but, in general, cost-benefit on other forensic means to capture data on crime and terrorist acts. For all the money you dump into a CCTV system, is that a really great payback, in the fact that you have a picture after the event? – Does anybody know of any studies that have looked at these contrasting –

MR. SLOBOGIN: There is quite a bit of research on CCTV. Probably the best-done meta-review of the effectiveness of CCTV showed that it had a very minimal effect on reduction of crime, about a 4-percent reduction in crime. There have also been studies in the U.K. that strongly suggest that having more cops on the street are much more effective than CCTV.

Also, over and over again we have heard how much the public wants CCTV. I think it's true that the public does, but its attitudes are a little bit more nuanced than what we've heard. For

instance, there was a survey done in the U.K., a country which, I think is fair to say, is more pro-camera than the United States, that nonetheless, found that 72 percent of the people surveyed agreed that these cameras could easily be abused and used by the wrong people; 39 percent believe the people in control of these systems could not be completely trusted to use them only for the public good; 37 percent felt that, in the future, cameras will be used by the government to control people; and more than 10 percent -- which isn't a huge percentage, but, nonetheless we're talking the U.K. here, not America -- believe there should not be any camera system at all. And this was without knowing any of the effectiveness research that we've been talking about.

There's also a piece of paper in your folder which is taken from some research I've done, which I think is relevant here. I asked people how intrusive they think various kinds of police investigative techniques are. As you see from this piece of paper, labeled Table 1 from the book mentioned earlier, I gave them 20 different scenarios. And one of the interesting findings was that the people that I asked -- there were about 200 people, randomly selected from the population – felt that monitoring over street cameras, which is what we're talking about, where the records are maintained for 96 hours was more intrusive than stopping drivers at a roadblock, by a very large margin. Well, if the Supreme Court thinks that roadblocks are a Fourth Amendment event, then, at least according to this survey, so should CCTV be a Fourth Amendment event, and it should be regulated. This is not to say the public doesn't like CCTV, but it is saying that the public thinks that it's intrusive and that, therefore, as a legal matter, it ought to be regulated.

And then, if you look further down in this table, you see that the survey participants felt that an overt camera system where the tapes are not destroyed is seen as one of the most intrusive scenarios, as intrusive as a search of a bedroom. So it's clear that, even though people may, in a general, vague sense, be in favor of CCTV, they see it as very intrusive, especially if the recordings are kept forever, because they see it as a seizure of what they're doing in the way that Deirdre was talking about, the permanent recording of their actions in public.

So, I think if we are going to legally regulate CCTV, as opposed to abolish it, this kind of public sentiment ought to be taken into account.

MS. LEVIN: But let me pose this. All of you are ivory-tower academics.

[Laughter.]

MS. LEVIN: And we heard, yesterday, from law enforcement people in the field dealing with crime every day, and they find that cameras and forensic use of cameras has been a really helpful tool. We heard from community representatives who say that their aldermen have been pushing to get cameras in their jurisdiction. And I know, when -- I don't watch too many crime shows, but, when I do, they're forever using cameras as a vehicle for finding the bad guys. So, for the bulk of the American public who believe that, "I've got nothing to hide.

The park is-- particularly when I go to the park, I'm not interested in hiding anything." Why do cameras pose a problem for you, either? What changes do you see it affecting, and why is there a different view from this panel today and the other panels we had yesterday?

MR. CARAFANO: Yes. My problem is if it's not the most effective use of money, it's not making people safer. And I go back to the forensic issue. I get forensic data from this film. Sure you do. Okay, fine. But would you better off with a system throughout your city that costs you multimillion dollars a year, or if you hired ten more CSI teams, would you solve more crimes? I don't see these kinds of discussions. This data is very anecdotal, and, to me, it's not terribly persuasive.

MS. MULLIGAN: Yes. We know there are a whole host of cognitive biases that force us, unfortunately, perhaps against our own will, to think things work. Right? If you look at the field of cognitive psychology, there are all different kinds of ways in which our experience of events and an actual study of what those events tell us end up being completely different things. And that's part of the reason that research is important, particularly when you're talking about the expense of billions of dollars of funding. And I didn't take any great comfort from understanding that CCTV cameras are another form of pork among aldermen. That really didn't make me feel much better about it. We're all familiar with pet-project spending, and we all, I think, agree that pet-project spending that doesn't go through the regular budgeting process is actually the worst kind of public spending there is. So, that doesn't make me feel good about it, it makes me feel worse about it.

But, I want to honor the goal of the program, which was not to debate the efficacy of CCTV. I think there is research out there. We're currently conducting a study, similar to what the Urban Institute is doing in San Francisco, that's looking at how are the cameras being used and the efficacy of the cameras. How does it play out in the context of investigations and in the context of prosecutions and for the defense attorneys? Because, believe it or not, the defense attorneys find it useful too; sometimes it can actually exonerate the person who has been accused of a crime.

So let's all assume that CCTV maybe, from a cost-benefit perspective, the right technology for the job. We've figured out that CCTV is really good for something, and it's better than anything else. Can we all go there and just accept that for one second? So, we also know that if we have this technology and we're going to use it, that it does raise some specific concerns. You know, saying that the police need not avert their eyes in a public place -- if you're walking down the streets, they come on -- that's different than saying that they can tail you all the time with a camera -- right? -- with a hidden camera. And so, how do we distinguish between the police not needing to avert their eyes in public place and them being able to single you out and follow you down the public street while you walk into your dentist's office or the abortion clinic-- you pick the place you don't want them to see you going. I think, if you look at some of the policies that are out there --and some of my students

put together a little compilation of some of the policies that police departments have adopted -- you'll see that there is some attention being paid to these issues. So, if you think about this ephemeral act going to this recorded act, I take some solace in the fact that some police departments are adopting policies--whether it's because they don't want to have to respond to FOIA requests or civil subpoenas, or because they actually understand that having 6 months of data about what the public is doing in the downtown area is a little overzealous, feels a little Orwellian. So, destroying that data when we realize it's not going to actually help us identify something that was criminal is really important.

Fresno, which is a city that we actually worked with, and the Constitution Project worked with, as well, they actually adopted this principle that says you have to have some kind of reasonable suspicion -- if Chris didn't mention -- well below the warrant requirement. Right? If you want to go into somebody's house, you've got to get a warrant. But if you want to stop somebody on the street and frisk them and pat them down to see if they have a weapon, you have to have some reasonable suspicion that this particular person is doing something wrong. And, in Fresno they're saying, if we're going to follow a particular person --not watch the general space, but we're going to zoom, pan, tilt to watch this person go down the street -- we want some kind of familiar test that we know, that we saywhen we single people out there's some constraint. It's not just who we feel like, and it can't be based, if you look at the park guidelines-- on race or religion or expressive activity. It has to be based on something that we would associate with criminal activity.

Now, as you tried to show us that perhaps singling out what are the three things that signaled terrorist activity -- I think terrorism, as Fred said, it's the worst-case scenario. If you think about the back-end algorithms people were talking about applying to the video feed, you need to be able to develop an algorithm that would identify a terrorist, what we know about terrorists. We think they're white; they're black. We think they're male; they're female. It's random, so far. We haven't been able to say: here's a profile of a terrorist that seems to hold up, which suggests that it's going to be really hard, through data mining or through video surveillance, to figure out who they are. And the other thing is there's nothing that a suicide bomber would like more than to have the event recorded forever. It's the worst-- suicide bombing as performance art.

And so, there is a little bit of a breakdown, if we think about its utility in those circumstances. But I think there are a bunch of rules that we could think about applying if there are instances where this technology meets the cost-benefit analysis.

MS. LEVIN: Well, in terms of those rules, I'm wondering, what about locations? We've talked about -- I think, Deirdre, you had talked about how this notion of temporal and spatial boundaries, and it is really put to the test as a result of the technology. Are there camera locations that everyone, sort of, agrees make sense, and even maybe cost-benefit sense? For

example, protecting critical infrastructure -- water treatment plants, chemical plants. Are there some areas where cameras make sense, from a legal and policy perspective? Jim?

MR. CARAFANO: Because something is critical infrastructure, that doesn't even come close to being a valuable criteria for determining whether a camera has an appropriate use or not. You have to go to, what is the use of that camera for?

I think some of the most obvious ones are mass transit systems. A mass transit system has a lot of people going through a lot of bottlenecks very quickly, and a problem in the system in one place could have rapidly cascading effects throughout the system. It's virtually impossible to have eyes everywhere in a system where you might have a critical node, where you might have a safety or a public safety concern or a transit issue, particularly in a subway, where you're in tunnels and stairs and everything. So, those kinds of venues are ideal.

Any venue where you have large amounts of the public moving through constricted spaces, and you have significant public safety concerns, and the notion of having personnel either there -- for example having a good vantage point in a subway tunnel is incredibly difficult. Having a good vantage point in in various parts of a stadium is difficult. So, those kinds of things, I think, are the kinds of considerations which would be primary.

Now one of the good things is, here is a problem-- one way to back away from the precipice of having to debate whether we need to live in a surveillance society or not was, if we had more fulsome discussions between public safety people and architects and planners when we built these things to begin with, you might limit the need for surveillance. I think stadiums and subway systems are good examples. Think through your public safety concerns, and maybe there are ways you can mitigate the requirement for surveillance, because you don't have the constrictions that create the massive public safety issues that you're worried about.

MR. CATE: To echo this, and to go back again to the question, I think it really highlights a critical issue that we've been overlooking-- in some ways, we've been overlooking, yesterday, as well -- and that is we need to be specific about what cameras are used, what their capacity is, and what they are being used for. So, for example, having a camera that views a crowd to determine whether you need crowd control, to determine whether you need to open exits, to determine whether you need to change the stoplight pattern in that road, is completely different from having a camera that will pan and tilt and zoom in, so that you can read somebody's text message. Completely different uses. And it is a grave error that I think many of us make to lump them all together into one common use.

So, for example, I would never answer your question the way that you might have intended for it to be answered, which is by saying, places, because it would depend on why we're putting the camera there, what type of camera are we putting, how is it going to be used? For example, we heard, yesterday, some cameras aren't monitored at all, but they are purely there to collect data after the fact, they're not designed to prevent a thing. Well, I wouldn't

put that anywhere, where prevention or immediate reaction mattered. That would make no sense in the traffic setting, where somebody needs to flip a switch and set the timing on the lights differently. Watching that tomorrow is no use at all. That doesn't mean I oppose cameras focused on traffic. It depends on what type of camera and how the system will be setup.

I think that the more specific we are, the more useful it makes the type of guidelines that people yesterday, and, I think, we today have been talking about, because it helps make those effectiveness determinations and appropriateness determinations more rational. So, "a" type of camera may make no sense in the public transportation setting; a "b" type of camera might be exactly what you need in the public transportation setting.

And so, similarly, we saw, yesterday, the clip in which we saw the masking of the homes. Well, that's a very important step. It's a way to try to protect privacy. I would wonder how many cameras we see deployed, in fact, have that masking. And is that masking appropriate in all settings? And, of course, the answer would be, of course not. There are places where you really do want to see, with great detail, what's going on. So, it's the specificity of the question, and then the breadth of the criteria, that I think are necessary to answer that question, that we really should be focused on.

MS. LEVIN: Well, I think now we've got three buckets of uses here that perhaps all too often we've lumped all together. We spent a lot of time yesterday talking about law enforcement. Counterterrorism comes up, but then is quickly dispatched because people say there is no evidence it works for counterterrorism. But then, what we've just talked about is public safety, and I don't think we really honed in on public safety yesterday.

And so, are those useful buckets? Are there other buckets that we should add to that list? And does everyone, sort of agree that public safety, there may be value to that, as part of the cost-benefit analysis? Is that a useful distinction between those three? At least we've got a beginning?

MS. MULLIGAN: Well, I do think it's really important to think about the various functions that police play. And I'll give you a -- for me, it was a really wonderful example. My students and I were meeting with the police officer in Richmond who's been tasked with developing the video surveillance privacy policies and policies, generally for a system that they're going to be putting in. And they have a big system going in at the port, because Richmond has a very large port. But they're also putting in cameras in their downtown, an area called the Iron Triangle, which has a huge murder problem right now. They have a huge crime rate, but murders in particular. And we were talking about different cities, different guidelines, what people were doing. And we were talking about monitoring during demonstrations. And that was an issue that people often thought about, in particular, in reference to places where people go to stakeout some kind of issue or whatever. And what was really fascinating is that, he said, "well, we have two kinds of demonstrations. We have

the demonstrations at the Texaco Plant. We're not putting any cameras up there; that's their problem. And we'll respond if they call us, but we're not putting cameras up there. And we're putting cameras in this downtown area. And the only kinds of demonstrations we have are these people that are basically trying to take back the city. And the demonstrations that they do-- they go to this really dangerous park and they set up their tents, and they spend the night." And he's, like, "They want all the cameras I can put to…" because it's the public safety mission that they're not feeling like they're out there doing anything illegal. The police couldn't possibly put enough officers down there to help these people feel safe. And he said, "You know, I'll talk with them about it, but my sense is that I don't want a rule that says we're not going to monitor demonstrations, because these people are putting themselves in the middle of a high-crime zone, setting up their tents, with their kids, because they're trying to take back their and my duty is to watch them." So, I do think it's very, as Fred said, specific to thinking about what's the purpose of the camera system. The purpose may not be singular, and it may change over time, but I do think, both from a perspective of thinking about the use of public funds, but also in thinking about what policies should be informing the use, even once the system is in, it may be fluid, it may not be a fixed instance.

MR. CARAFANO: If we move towards regimes that move more towards community-based policing and, problem-solving policing, and you had to develop a strategy, and then you're identifying the context in which these resources are being used, and then you can have the kinds of transparencies and controls you want. But if you just create a reactive system, where, in a sense you're just putting a bunch of eyes out there, and then, later on, you're determining how and why you're using that information, that is much more likely to have a a problematic situation. You're much more likely to move down the slippery slope of doing things that are inappropriate.

MS. LEVIN: Well, it sounds like you're talking about putting some switches on the cameras that people can make decisions about when to turn them -- if they're -- once they go -- the initial steps of explaining the use, and justifying it, and that its purpose, and there are guidelines in place, it allows you to turn the switches on and off for very specific purposes and uses. It's not just: buy the cameras and put them up.

MR. CATE: Well, or it may mean buying the right cameras.

MS. LEVIN: Or the right cameras.

MR. CATE: In other words -- and that's actually, again, an important resource issues. You may not need the $100,000 camera, where the $5,000 camera will do, if you don't need all of the zooming and remote access and ability to move the camera.

Another, by the way, bucket of these uses I think's important we put on the table is for both accountability and the protection of public safety officers. And so, therefore, having a camera in the patrol car, so that when the officer approaches the stopped car -- it may serve

incredibly important uses that have nothing to do with what we've been talking about, so forth, in terms of helping there, we do already have some suspicion articulated; for some reason, the police officer has pulled over this car, and what we're doing is building a record that may be useful subsequently in the prosecution or in the defense or in the protection of that police officer.

MS. LEVIN: I do want to raise another question, which was touched on a little bit, but I'd like this panel to discuss what are the rules or guidelines or limitations with regard to government access of private-sector camera data? We know that there are a lot of commercial operations that use cameras to protect property, and for the safety of their employees and customers and all of that, or companies that protect property through their use of cameras. What about government access and use of this information?

And I think we heard, yesterday, from at least one community where there's actually, a relationship between the community law enforcement as with the private-sector holders of the cameras. And what about this relationship, and are there any rules that should apply?

MS. MULLIGAN: I think all of us were quite uncomfortable -- we all know that the wall between the public and private -- with respect to the Fourth Amendment -- is a rather porous and, perhaps increasingly plowed-under wall. The ability of government to access anything that's contained in what are called business records generally falls completely outside the Fourth Amendment, although several of us think that that's an overreaching of the existing court cases.

In the context of the video surveillance tapes, I don't think that, one, people can turn them over to the police, and, two, that the police can request them, and that that would likely be found to not raise any Fourth Amendment issues, generally, when we're talking about a business's tapes of what was happening in its store. But I do think there's this disease with saying that the police department is going to have a live feed of everything going on in every downtown shopkeeper's store. And I've spent a fair amount of time working on electronic surveillance issues, and there's been lots of questions about whether or not the government can basically require the telecommunications providers to design their systems to make them wiretap-able. And, yes, of course they cooperate with law enforcement when they come in with a request for information, but can we proactively tell them that they have to design their systems so they are wiretap-able?

I think there's a really interesting lack of parallel here. It seems that, basically, the answer is, "yes, we're going to design our stores now, perhaps, because it's required if we want to build in a given area of the city, where the police are going to be able to monitor everything in the store as a condition of us having a store." That's really an interesting flip, because tradition -- it's not that government can't get access to what records the private sector has, it's that we don't assume that the government is going to routinely access all the things that are happening in the private sector. You think about the total information awareness pushback,

that we're going to dump all of the records over. And here, we're not dumping them, it's going to be a live feed. And so for me, I was, like, wow, that's just a very different framework for how we think about the relationship between private-sector record holders and the government. I have a feeling it triggered similar thoughts from some of my colleagues.

MS. LEVIN: But, in the homeland security area, we often view relationships, partnerships with particularly critical infrastructure, but with businesses as a part of the way in which we help protect the homeland. So, in that context, it may not be so foreign.

MR. SLOBOGIN: Well, it still should be the case, as you were just saying, that the government shouldn't have open, comprehensive access to everything that private entities are discovering through their surveillance. There ought to be some justification before the government can access this information. A Supreme Court Justice wrote: "The interest in not having public activities observed and recorded may prevail in the absence of any governmental justification for the surveillance." Guess which Justice wrote this? Rehnquist. Even he apparently felt there needed to be justification for this type of activity.

So, what type of justification would be required? If there were an incident in a store, certainly government could get access to the surveillance tapes. But 24/7 access to private-entity tapes, just because the government wants it? I think that goes way beyond any reasonable justification for government access to the information. I thought it was interesting that, at least originally in Baltimore, access to tapes was not permissible unless there had been an incident report. There, you obviously have reasonable suspicion, or maybe even probable cause with respect to what may be on the tape.

Another possible situation, though I'm a lot more ambivalent about this, was mentioned yesterday– the situation where you have an area that's clearly a high-crime area, where a large number of crimes are being committed. That might be another situation where it's justifiable to put up CCTV cameras, though, even there, there maybe limitations on when the cameras can be turned on and off, depending on what the pattern of criminal activity is. I agree with Jim that just saying something's a "critical infrastructure" doesn't necessarily justify that cameras be placed there. It depends on what you mean by critical infrastructure. And there needs to be some kind of showing that it's critical, and that it's threatened by some objective threat.

Yesterday, we also heard mentioned the need for cameras in order to monitor protests. Why? I don't understand, necessarily, what the justification is in that situation, especially when you consider the chilling effect that people who are engaged in the protest will feel when they see cameras trained on them and know that everything they're doing during the protest is being recorded. There are some very interesting labor-law cases decided by the NLRB, the National Labor Relations Board, which holds that it's illegal to train cameras on employees who are striking. I think the rationale for these cases is that there's a fear that freedom of

speech will be chilled if employers use cameras in this fashion. I think the same rationale applies, generally speaking, to protests. Now, if there's a specific reason, a belief that there might be some kind of dangerous incident occurring during the protest, that's arguably a different situation. But, just because there's going to be a demonstration going on, it's okay to have cameras? No.

I think there need to be specific justifications in each of these situations. That's, I think, what the underlying policy of the Fourth Amendment is, and what the underlying policy of the other constitutional principles I mentioned is as well.

MR. CATE: Yes, let me say, again, thinking on the much more practical side, I would be scared to death, if I were a business, giving the government unlimited access to my video feed. You just have to look in Congress right now, where our Nation -- America's telecommunications service providers are fighting 40 lawsuits by trying to seek immunity legislation. If they fail -- again, according to this morning's newspaper, where I did all of my research for this panel –

[Laughter.]

MR. CATE: -- their very existence is threatened. So, is that the situation you want to be in? It comes back to written guidelines, written agreements. If you say, "we are providing access for these purposes, subject to these limits, subject to these protections," this will highlight exactly where the rub is, because industry's going to say, we want the government to immunize us. Police department's going to say, "we can't immunize you. We don't know what legal authority we have for this, we're certainly not going to cover your losses in this, too." Now you're going to have the issue right on the table, where it needs to be. What's the authority for this? Where's the clear legal authority for this? And how are those losses, when they occur, going to be determined?

MR. BLITZ: I gathered, from the discussions yesterday, that one of the reasons that law enforcement has these partnership arrangements with private entities is just that it's, in some cases, a cost-effective way to cover more public space, so that, in some cases, rather than wanting to tap into the video feed from inside a store, they just want to see the parking lot, or they just want to see the street outside. So, in a sense, they're doing what they do with government-operated cameras, they're just doing it with the help of private entities. And if that's the case, then, I suppose, under existing Fourth Amendment law, most of the footage captured by the cameras will probably be outside Fourth Amendment protection, for the same reason it is when the government captures it.

At the same time, to the extent that we believe that there are privacy concerns with what cameras capture, even in public, even if you believe that cameras are effective, that they serve invaluable purposes for law enforcement, there are still these privacy concerns, one being that they capture intimate behavior like going to the doctor, showing affection, things that we

can't help but do, even in public, at least in a free society -- and that, also, even when one's not engaged in such behavior, it's just very unsettling to be the subject of constant or intense surveillance. That's true, whether or not it's happening right outside a private entity, or whether it's happening from a government camera. So, I don't see any reason why, if that information has to be collected, it should be treated differently, or shouldn't be subject to the same masking technology or the same limits on dissemination to third parties, that would apply to the information collected by the government's own cameras.

So, this is not really an argument that information should never be collected or never be shared, but, to the extent we recognize the need for privacy and civil liberties protections for the information collected by public government-operated cameras, it seems those same limitations should apply to feeds from private information -- from privately operated cameras.

MS. MULLIGAN: Yes, I certainly want to acknowledge we had a conversation with Chief Keyes about the Clovis cameras, and it's very clear that the cameras that they're putting in are to view the outside space, not to view inside the store. But there are other jurisdictions doing other things with their requirements.

But I do also want to, kind of, highlight the fact that once you delegate these activities outside the police department, there's also a question about what kind of obligation you have to ensure that those cameras are not misused. If you've directed that stores have to deploy them for police use, how do you make sure that they're used in a way that's consistent only with the policing function? Clearly, it would be hard to tell Wal-Mart or Target that they can't use them for their own internal security, but I think there's a question about what kind of auditing and oversight obligations you take on with respect to making sure that, you know, they're used in a way that's consistent with the direction that you were seeking when you told them they had to do it.

You wouldn't want, by delegating the activity outside of the police department, to basically delegate away the responsibility for making sure that they were used in a way consistent with the community's values.

MS. LEVIN: Well, now that we're, sort of, talking about the accountability and what the rules might be, I'm interested in hearing from our panelists about -- again, assuming the cost-benefit analysis in favor of a use of camera -- cameras, in certain situations-- what are the recommendations, the policies, that you think need to be put in place with regard to protections so that privacy and civil liberties concerns are addressed? And I'm talking the whole range of retention, notice, all those other related areas.

MR. BLITZ: Well, some of the things are things that we heard a little bit about yesterday. So, we heard both about technological protections for privacy, which include masking, not just of houses, but also of individual faces, and also institutional protections of privacy, like

policies that mandate that records not be kept longer than a certain period of time, that there be stringent protections against release to third parties. And I think that one can raise a couple of questions about these two forms of protections. One, which Chris has already raised and I think is worth a great deal of thought, is, where do you place them in the legal and administrative framework that governs video surveillance? Are they simply going to be guidelines? Are they going to be administrative rules? Or are they going to be actually in legislation? I think Chris gave some compelling reasons for why you actually might want them in legislation rather than simply, say, in the form of guidelines.

Another question one might raise is -- given that a lot of the concerns that people are raising about the use of video surveillance apply more to the advanced technology that goes with it -- so, for example, to the analytics that might be done to track someone in recording after-the-fact, or to use face recognition, or perhaps what's more feasible now, license-plate recognition after-the-fact to identify someone -- can you use certain protections, maybe even a warrant requirement or some other process that meant – that embodies an individualized suspicion requirement to make sure that that sort of more invasive look at the records captured by these cameras doesn't take place unless it really needs to take place, even if you can't insist upon a warrant for the initial observation? Alright? It may be that, look, these cameras are up. If it's a 24/7 system, of course you can't insist upon a warrant. The point of having these cameras operating is precisely that they capture information that no one knows ahead of time, that you'll need, but you may still be able to have protections requiring a review by a neutral magistrate or by some other official, to make sure that more detailed analysis or identification of an individual or tracking of an individual doesn't take place unless it really needs to take place. That's one concept that I think should get a great deal of consideration as these systems are put into place, and as people give thought to the kinds of rules that should govern them.

MR. CATE: Here's my list. First of all, I wouldn't spend money on any new technology without having a clear written purpose for why I'm doing it. Frankly, I think that needs to be adopted at a fairly high level, because elected leaders have a tendency to run and hide when the flack starts to fly, and that it is better to have had a higher-level signoff, so that if you do it at the police department level, it's you want to get it as far up the food chain as possible, so somebody says, "yes, I have looked at this specific analysis, I know why they're being used, I know the type of technology we're putting in place to accomplish those purposes. That's appropriate. And I'm making this finding, on the record, supporting that." That way, for people in the trenches, it means you're going to have support when you need it, and you are going to need it. For privacy concerns, it means you're getting an evaluation in advance.

I think you then need at least two sets of features to deal with the types of issues we've been talking about. One is to specify the technologies you're going to use, the technology protections. So, if that's masking, that's appropriate; if that's automatic audit records so that

you generate a trail of who's accessed the records -- there would be many examples of this; I don't want to take the time to belabor them all.

The other, of course, is policies, so that you have policies about who gets access for what purpose, how long you retain the records, and so forth.

Then, on top of this -- I'm sorry, there's more to come -- you need some sort of clear oversight system. Now, to my mind, that would mean, at a minimum, you want reporting. In other words, you want whoever is responsible for this to be reporting up the food chain, on a -- on a quarterly or semiannual or annual basis, about how it's working, where there's need for change, and so forth. You also need some sort of clear oversight. Who has the oversight? Is there an inspector general? Is there a commission? Is there a city council?

I think auditing for compliance is critical, because nobody's going to believe your self-assurance that you obeyed the rules. It's not because we distrust you, it's because the public distrusts all of us who work in the public sector. And so, auditing that goes in and says, "we have matched the access records with the policy" -- on a selective basis; I'm not talking about a comprehensive audit, but a selective audit -- so that there is a way of verifying externally, from a different entity -- in other words, a different entity within the government or an outside entity -- that these rules have been complied with.

There has to be enforcement. And, again, enforcement doesn't mean gratuitous enforcement. I'm not suggesting enforcing, just to show you can enforce. But it's difficult to believe, as these cameras proliferate across the country, that they are all consistently, uniformly being used only according to appropriate policies.

Just two final points. One is, there needs to be some way of, through this process, building in public transparency. I'm not a huge believer in notices. In fact, I think they're a tremendous waste of time to give people notice when there's nothing they can do about it. So, therefore, the British model of "CCTV in Use" slapped up on every wall you pass -- I just don't see it as anything other than graffiti.

On the other hand, notice can serve important public transparency roles, and I think that is useful to think about how much of this can be made public, to what extent should the public have access to these records, to the audit report, to the guidelines, and so forth? I would obviously favor maximum access and some forms of moderate or appropriate notice, so that people are at least aware that there may be issues they want to -- that they want to deal with.

And then, on top of this whole system, I think there needs to be some awareness that change is inevitable. So, frankly, in some ways, that's what worries me the most about video surveillance, just speaking personally. That is that the technology just gets better and better, and more fabulous, and more potential for intrusiveness. And so, the types of policies, the types of guidelines that we might use to deal with cameras that can look at a broad crowd, but they're fuzzy pictures, so you can't pick out faces and so forth; once we combine audio,

video, other types of sensory monitoring, types of data analysis that automatically process the digital images, I think this may very well require reviewing these policies and technologies and so forth. And so, the danger is, here – and we all run afoul on this danger – that we put in place the perfect system, but, of course, it's out of date in, you know, 12 months, and we're so happy we have the system that took us 5 years to get, we don't want to ever revisit it again.

MR. SLOBOGIN: Yes, I'd like to follow up on that. We are, supposedly, the legal panel, as opposed to the policy panel, so I basically want to echo –

MS. LEVIN: No, no, law and policy.

MR. SLOBOGIN: Okay. Well, then I'm going to focus on the law part of it. I think that everything that Fred and others have said can and should be justified on a legal basis, looking at Fourth Amendment doctrine, and, again, focusing in particular on the roadblock cases. The Supreme Court's made it very clear, with respect to justification of roadblocks, that a roadblock can only be set up if a "politically accountable official" -- that's the Supreme Court's language -- a politically accountable official has said that the roadblock is positioned in an appropriate place. That echoes what Fred was saying, that you need a very high-level individual making these kinds of decisions. I think the same thing should be said about CCTV.

Also in the Sitz case, a sobriety checkpoint case, the Court made very clear that, even though it's typically going to be up to the politically accountable official as to which alternative, among reasonable alternatives, law enforcement goes with, determining whether alternatives are reasonable is ultimately up to the courts.

MR. SLOBOGIN: Additionally, with respect to the notice issue, the roadblock cases make it very clear that, in order for a roadblock to be valid, there has to be notice to the public that the roadblock is taking place. And there are a number of reasons the Court gave for that, including showing the public that these are duly-authorized law enforcement techniques.

In terms of storage and dissemination, the Supreme Court has said in Whalen v. Roe that, under the Due Process Clause it's incumbent upon government to ensure the security of records. In terms of revealing information to third parties, in cases like Wilson v. Layne the Court made clear that there cannot be gratuitous disclosure of information to third parties, even to the media; law enforcement has an obligation to keep this information secure until there's a bona fide law enforcement interest in disclosing it.

With respect to accountability, I want to echo again what Fred was saying: There needs to be a justification for a CCTV, continuous justification. You can't just justify it on the front end, and then say, "Well, for the next 30 years we're going to allow this to happen." This is different from the typical search, which is a one-time event, a search of a house or a car, what have you.. This is continuous searching, so there has to be continuous justification, there has

to be periodic review, there has to be proof that the camera system is working, is accomplishing the goals that have been setout at the outset. And then, if there's no justification, the system has to be ended.

MS. MULLIGAN: I'm going to out myself as a process geek. I think there are several buckets. There's transparency, and, with respect to the transparency issues, the privacy impact assessments-- and Dan Sutherland said they're working on a civil liberties impact assessment -- I think both of those --we know the privacy impact assessment, at least as performed by DHS, have been really important decisional tools in thinking about the relative intrusiveness of different technologies, and I actually think, in many ways, a backdoor into the cost-benefit analysis that many of us would like to see, because they force agencies to rationalize their decisionmaking and to consider alternative technologies. I think those process-based tools, if they're used by experts, not just by somebody who doesn't know much about the technology, but it has to be with somebody who actually has, kind of, a field expertise, probably in privacy, as well as enough technological sophistication to know what's available with respect to technological mitigations or alternative choices. I think this is where you get, kind of, an -- the exhaustion or least -- Dan Sutherland mentioned trying to force the use of the least-intrusive technology or the least-restrictive. In a First Amendment law, we think about the least-restrictive. So, is there a way for the government to do what it needs to do here in a way that does not intrude on other interests? I think that the privacy impact assessment and the civil liberties assessment, as decisional tools, can help us in formulating those questions and move us towards better answers. I think the work that your office has done, and that the Civil Liberties Office is doing, is incredibly important and would be really useful, and I'd like to see folks using those tools.

Now, those tools, though, need to be used in a way that allow the public, before the technology has been invested in or money to purchase it has been acquired, to comment and to participate. This is about community policing, it's about use of scarce resources. I don't know any police department that has more money than it needs. I think it's really important that the transparency aspect is both about how decisions are being made, but also allows the public to review those decisions before funds are allocated or funds are even sought. I think that's an incredibly important process.

The Constitution Project has focused a lot on public participation. I know we're going to hear more about this from the ACLU. I think those are really important issues.

Checks on power. I think that there have to be rules that limit discretion, and I think those can be things that if you want us --so, in many other jurisdictions -- if you want to access stored footage, you don't go down and riffle through it at will, right? You have to say, "here's why I want to access the footage, and here's my purpose, and here's the -- I want footage from this time period and from this location." And that's because we don't want people to just, kind of, randomly perusing stuff to look for cute girls.

I think checks on discretion are important, but I also think checks on discretion can be built in with the technology itself. There are all different kinds of technologies that allow us to detect different kinds of events, whether it's somebody moving across a line in the sand or going over a fence. Yes, we can use video surveillance to detect that. We can also use motion sensors. And so, thinking about, what's the least information we need to perform the task? What's the trigger here? Do I really want to see who's going over the fence, or do I want to know that somebody just climbed over the fence? I want to know somebody climbed over the fence, so let me use a technology that's way cheaper, and also doesn't give me all this extraneous information about who it was and what color they were or whatever. So, I think that discretion can be limited, both through technology and through policy.

Certainly, the rules that are in place in jurisdictions that limit the kinds of information that can be used to determine when we follow somebody, so, raise expressive activity, you know, thinking about that those can't be the sole purpose for singling somebody out. Those are, again, really checks on power.

Checks on mission creep. Really important. If you build it, they will come. Who will come? Other agencies. Who else will come? Civil litigants, in all sizes and kinds. And thinking about data retention as one way to prevent mission creep is really important. So, destroy information -- and, you know, talking with Richmond, they were, like, "we know, in 72 hours, whether or not a crime happened. So, if we're not, you know, flagging the stuff to keep, we're going to get rid of it." I know, from other jurisdictions, like San Francisco right now, data retention initially 72 hours, then it went to 7 days, now it's 7 to 14. The public defenders are actually coming in and saying, "we want you to hold data for 21 days," because, from their perspective, they might need it as exculpatory evidence. But thinking about data retention, if the data doesn't exist, it can't be repurposed. That's very important.

Thinking through the Public Records Act request, very important. Although I do want to flag the transparency issue. Yes, the notices that say, "you're under surveillance" might not be so good. What we did in Berkeley, we actually put an image of what was being watched. It was really – "hey, that's me. Is somebody following me? Wait. Wait a second." And so, there are actually ways to use this technology. If you're going to put it up in the police department, and allow, as Chief Keyes said, the public can come in and see what it is we're watching. Well, you can also put a visual display in the downtown area so people can see what you're watching. And many people are big fans of this "sousveillance," right? "I watch you, you watch me." And certainly puts a lot of check on police discretion if we know what they're doing. Now, it may make the technology less effective, I'll admit that. But, you know, transparency can be useful, and we think about it in ways other than having a notice up.

I also think, certainly, auditing, oversight, and accountability are critical here. External oversight, I think there has to be some form of external oversight. Audits have to be built into the technological systems, as well as the process systems.

And then, finally, on accountability, it's not just, "is the system being used as it ought to be?" but it's also, "does the system work for the purposes that we chose to deploy it?" I do want to credit, you know, San Francisco right now, at the, kind of, pushing of the police -- the Police Oversight Board has said, "you actually have to evaluate the system." I think accountability is not just making sure that we're using it as we said we were going to use it, but actually making sure that we should continue using it at all. Is this doing what we wanted it to do? -- as an important component of accountability.

MR. CARAFANO: Yes, I agree with all of this. I think what I would not do, though, is use homeland security grants to drive what systems people adapt and the policies they adapt. I think that hasn't-- that's problematic in a number of ways. I think it's problematic from a federalist standpoint. I think it's problematic, in terms of keeping up with technologies and everything else, but, you know, allowing, kind of, States to adapt and innovate and keep it in the marketplace. I also think that it's incumbent upon the user of the system, the creator of the system, to ultimately have responsibility for what they do and what's being done. So, I don't think that, in a sense, I would have the department try to drive the behavior. I'm a fan of the critical capabilities list, and I think that that's a legitimate notion, is that, describing a national response and preparedness system, and then describing, articulating what legitimately is seen as the States' role, what the critical capabilities are, and requiring that, if they use Federal money, they spend it on the critical capabilities and they identify what critical capability they're filling and how they're filling it. I think that's perfectly legitimate. But, in a sense, dictating this, kind of, litany of requirements through the grant system, "you can't have money for a TV system unless it has all these things in it," I don't think I would do that.

Now, what I think is a better vehicle, and perhaps it would have enormous utility, is the Safety Act. I mean, if the Department of Homeland Security wants to certify a technology under the Safety Act as having a number of attributes, from auditing -- immutable auditing to whatever -- and States or local governments choose to buy from vendors that provide that good or service, I think that that's fine, and that, you know, there are immunity protections under the Safety Act, and I think that's an existing vehicle, it's a much more appropriate vehicle, and using grant guidance is probably not the most appropriate vehicle. Certainly, providing some kind of immunity protection or -- that, I don't think is appropriate, either, through the grant system. I don't know if other people disagree or –

MS. LEVIN: I want to ask one more question, and then I want to open up for comments. And I know, Don, we want to hear you respond to some of the points that were made.

And that is, we've talked about accountability and enforcement if we have guidelines, how do you enforce guidelines and where are the costs going to -- what are the costs for enforcement and accountability, and does that get built into the cost-benefit analysis, too?

MR. CARAFANO: It should. Right? It's part of the cost of running the system.

MS. MULLIGAN: And the cost of responding to subpoenas and when you build a system, there's costs you can control and there's costs that you should reasonably foresee. I think that, you know, a responsible agency takes all of those into account.

MR. BLITZ: I also think one has to think about the risk of not having all those protections in place. And one high-level remark is useful. I think it's useful to acknowledge one reason that --I'm guessing that in a lot of the cases we heard about yesterday, the public seems to support use of video surveillance. One intuition which I think everyone on the panel agrees with, although I'll be corrected if I'm wrong, is that nobody wants the police to be left with primitive technology when criminals and terrorists have access to more sophisticated technology. I think Deirdre's comments about possible alternative sophisticated technologies highlight that. But I think that's probably one thing that's going through the minds of people who support expanded use of CCTV; they don't want police to be deprived of an important tool and technological development.

Another important intuition which has power for people, and, I think, has power for me, is, even though people will, upon reflection, admit that there are lots of things they do in public that they would characterize as private, that they don't want to be available to the world, we *do* often share private information, that we wouldn't share with anybody else, with certain types of people. So, for example, when we go to a doctor or a psychiatrist, or we go to an attorney, we'll tell them many details about their lives that we won't share with other people, sometimes even with people in our own family, our own local community. I think there's a parallel to the way that some people are thinking about video surveillance as it was described yesterday. Given the assumption they'll make that there's certain information about what they do in public that they're perfectly willing to share with the police for the job that police do.

The same way that you'll share health information with a doctor, because the doctor needs that information to protect your health, you're willing to share a certain information about what you do in public that they would rather keep private, they're still perfectly willing to share it with the police for the job that police do. But, if you think about that analogy -- to doctors, to attorneys -- in all of those cases that I can think of where you share information, medical information or other private information with a certain type of person, you do so under the assumption that there are stringent privacy protections in place that will kick in and give that person very, very strong incentives not to cross the boundary line, not -- I know, you know, as an attorney, if I e-mailed confidential client information, if I forwarded a

confidential client e-mail to someone, that wouldn't be very good for my job, and I wouldn't only be in trouble with my firm, I would be in trouble with the profession.

I think that the same kind of reassurance is necessary when we share information. It's not that we shouldn't share this information, or that we should take all the cameras down, but we have to assure that there are similar protections in place so that police can do their job, but we can have assurance that this information won't go from the police to all kinds of other actors that might want it, and also won't be used by the State for all kinds of other reasons. And that, even if people aren't thinking about it now, I think that'll affect public support for these systems in the future, and probably will require, not only that there be some statements and guidelines, but that there be, as there are for doctors and for lawyers, public rules – in some cases, statutory rules – that are designed to protect the privacy and to hold accountable those who don't protect the private information they have, or don't take into account the civil liberties concerns that are relevant.

MS. LEVIN: Okay. Alright. We have time now for questions. And I'm going to start with Don Zoufal, who was on our community panel yesterday.

MR. ZOUFAL: I have just two questions. One is, after all this discussion, I remain confident, at least from my own research, that there isn't a Fourth Amendment case that precludes the use of video in public space, that it's not a search with -- as that's defined. And, I know, Professor, you talked about Sitz and Edmonds-- but those were seizure cases, not search cases, and there's a different jurisprudence, I think, with regard to seizure than there is with regard to search. So, I guess the question is: is there a Fourth Amendment case that tells me that I can't do this?

MS. MULLIGAN: I think we've all said that there isn't a Fourth Amendment case on point that says you can't do -- now, I don't know exactly what you are doing -- right?

[Laughter.]

MR. ZOUFAL: Surveillance -- the question is, surveillance -- you know, video -- CCTV surveillance --CCTV surveillance in the public space has been around forever. We've been –

MS. MULLIGAN: Yes.

MR. ZOUFAL: -- surveilling parks, we've been surveilling streets, we've been surveilling high-crime neighborhoods, we've been surveilling buildings, we've been surveilling airports, we've been surveilling arange of things. So –

MS. MULLIGAN: Yes.

MR. ZOUFAL: -- this isn't really a new discussion, and it is something that there's mature jurisprudence on.

MS. MULLIGAN: I think we all agree that the look and feel of surveillance is often really significant in how the court understands it. And so, one of the things that I think is worth considering is, if you think about what we're talking about is enhancing senses, right?

MR. ZOUFAL: True.

MS. MULLIGAN: I spend a lot of time with scientists. When I explain to them, well, yeah, if you want to use a hyperbolic mike in a public place, you could be in trouble, but, you know, use whatever kind of night vision you want. They're, like, "that's nuts." It's nuts, as a technical matter. "So, I can -- how about smell?" they say, "Can I enhance smell?" "Well, if you use a dog, because it's the perfect technology. It's not even a search." Smell whatever you want, even sniff around in a private place -- right? -- bring it around the car. And so, we have this schizophrenia right now in how we think about enhancing senses, where some senses, it seems we can enhance without limit, perhaps. What I would suggest is that I think, no, maybe we just haven't found the limit.

And certainly, we know, with respect to the Kyllo case, there was a limit. So, some people would say, "Well" –

MR. ZOUFAL: And with the Tobias case, there wasn't.

MS. MULLIGAN: Exactly, yes. And you can say the distinction was the house versus the public place. And I can also say, perhaps it may also be the extent to which people view the technology as not just enhancing what we do, but actually qualitatively shaping of the kinds of –

MR. ZOUFAL: Or –

MS. MULLIGAN: -- surveillance. I think that what all of us are trying to say is that it may take quite some time before have the form of surveillance that would get a court case that said, "now, that's not okay," but that -- you know, that we think the real development shouldn't be waiting for the court case.

MR. ZOUFAL: Or to default back to, really, what the standard is that seems to have been set, which is reasonable expectation of privacy, and that the notion is, on the olfactory side, people don't really seem to have that -- or, at least at a certain level, don't seem to have that expectation. Or maybe it's that they don't have an expectation of possessing contraband, which, I guess, is really the ultimate issue there. So, if we could make -- and I guess that's a second question, is if we can make technology more binary, and then deal with the false-negative/false-positive and –

MS. MULLIGAN: Absolutely. I mean, the court cases-- if you design a test that only says, is the substance cocaine –

MR. ZOUFAL: Contraband or not.

MS. MULLIGAN: -- or the perfect dog, right?-- which, all dogs are apparently perfect

MR. ZOUFAL: Which none -- well.

MS. MULLIGAN: -- which says, no, we only smell for drugs, it's not even a search, right? Just forget about it. That's fine. And I do think that there is –

MR. ZOUFAL: No, it's -- well, yeah, I guess technically –

MS. MULLIGAN: Yes.

MR. ZOUFAL: -- it's not a search, because the notion is –

MS. MULLIGAN: It –

MR. ZOUFAL: -- there's no reasonable expectation –

MS. MULLIGAN: Marc Eckenweiler is nodding his head back there.

MR. ZOUFAL: -- of privacy in contraband. Well, because there's –

MS. MULLIGAN: No –

MR. ZOUFAL: -- no reasonable expectation of privacy in contraband.

MS. MULLIGAN: You can justify it, but that no search has occurred, because you had no reasonable expectation of privacy in your contraband. And so to the extent that we can design -- and this is one of the things I talk to my technologists about -- if you design perfect technology, searches may never occur under the legal framework. Kind of fascinating thing, as a conceptual matter –

MR. CARAFANO: Yeah, but, I mean –

MS. MULLIGAN: -- right?

MR. CARAFANO: -- but this is where you get directly to the practical issues. You drive down false positives as you drives up false negatives as you drive a system that's perfect –

MS. MULLIGAN: There is no such thing as a perfect technology.

MR. CARAFANO: Right, that's exactly right. But, you know, you drive up the cost, and that's where the reasonable question is, is, What are you reasonably trying to do here? That's what I often think is the issue, is it --the discussion -- we could have a fascinating discussion about the limits of the law, but we should have a much more fascinating discussion about what's practical and makes sense and is cost-effective.

MR. ZOUFAL: Right. I guess the ultimate issue is trying to separate two from -- the legal issues from the policy decision issues of: I'm trying to weigh these things, and do I want to put up CCTV camera, or do I want to have another officer, or do I just do nothing? Or -- or pick another range of alternatives – covert surveillance, cars, or however you want to do it.

The point is, though, that, even if CCTV isn't a perfect substitute for these other things, it may be the cost-effective one, it may be the best that we can do with the technology that we have, with the personnel we have, and with the resources we have. Ultimately, that seems to me to be a decision that the policymakers need to make.

I guess one thing, Deirdre, that I had, in terms of your comment about aldermen and pork, the point wasn't that it was a pork program, the point was to give them the opportunity to meet what they felt were community needs. They had communities that wanted to have these cameras in park areas or other areas around the city, or where the community felt it was important. If you want to engage in the community portion of the discussion, then you have to engage in the community portion of the discussion, and you have to rely on their judgments. And it seems to me that, significantly, their judgments are that these cameras do make them safer.

Now, whether you'd argue whether that's a fully informed decision, I don't know, but it seems to me the general premise that they're starting with -- and I haven't seen anything that really undercuts the kind of commonsense notion that they're willing to make some tradeoffs about that -- the privacy issue that you say doesn't resonate with some people in a park, but resonates with you, butwe have to make accommodations what everybody wants in the park so that we can have more people using it.

MS. LEVIN: Alright, we're going to --Deirdre, do you want to respond? And then we're going to go on to the next question.

MR. ZOUFAL: I'm sorry.

MS. LEVIN: Thanks, Don.

MS. MULLIGAN: Debates about public spending and, you know, set-asides for legislators -- just as a general matter? As a general matter, it allows for people to get pet projects, and perhaps to have less-rational, well-reasoned expenditures of public funds. And we know that it occurs for all different reasons. But, specifically when we're talking about technology, which is sophisticated, it makes sense to have people with expertise asked to think long and hard about whether or not it's the right way to spend money. I don't think allocating those decisions, "the public wants it, therefore we should give it to them," is the best way to spend our public money. And it may be okay, because giving the people what they want gets people reelected, but that doesn't necessarily mean it provides us protection. If the question here is, "is that a good way to provide protection?" I would guess not.

MR. CARAFANO: It does get you a 700-mile wall, though.

MS. LEVIN: I'm sorry, we should have what?

MR. CARAFANO: It does get you a 700-mile wall. So –

MR. ERICKSON: I'm Stan Erickson, NIJ.A question about the coupling of audio surveillance with the visual surveillance. I think you initially mentioned that there were special constitutional limitations on that. And my, sort of, narrow question is were those limitations specifically sufficient -- specific that they referred only to speech -- recording of speech, or was it a term that you used audio surveillance covered, in general? And so, these types of couplings of audio surveillance systems, like gunshot detection systems with cameras that focus in on the subject area, does that set a constitutional problem or not?

MR. SLOBOGIN: What I was referring to was speech. Both the Constitution, as interpreted in Katz, and Title III talk about communications which are associated with the reasonable expectation of privacy. And Katz stands for the proposition you can have that expectation of privacy even with respect to public speech. Not always, but certainly sometimes. If you reasonably expect a conversation to be private, there would be constitutional recognition of its interception.

As to the gunshot scenario, I think you could make the argument there is some protection there, as well. But I think that probably falls under the category that Don was talking about. Yeah, it's very expressive speech...

[Laughter.]

MR. SLOBOGIN: …but the chances are very high that the gunshot reflects illegal activity, and therefore, discovering only that information would not be a search under the Place/Caballas kind of reasoning because the only information you're getting has no privacy significance –

MS. MULLIGAN: But the gunshot –

MR. SLOBOGIN: -- because it's associated with crime.

MS. MULLIGAN: -- technologies actually don't only pick up gunshots.

MR. SLOBOGIN: Nope, that's right.

MS. MULLIGAN: Yes.

MR. SLOBOGIN: But if they did only pick up gunshots that would be part of the analysis. So it may be hard to argue the Fourth Amendment applies in this particular case. But the reason I think the roadblock jurisprudence is relevant is that it establishes that the overarching consideration under the Fourth Amendment is the relative degree of intrusiveness. And, at least according to my survey, people see CCTV as more intrusive than a roadblock, so it's arguable that the Fourth Amendment should apply in most situations involving CCTV.

MR. BLITZ: One really quick interesting twist on this. If there's the sort of protection that Chris was talking about for communications picked up in audio surveillance, one might ask

whether or not certain forms of visual surveillance ought to be covered by the Fourth Amendment, for the same reason --for example, lip reading, books, letters, et cetera --and whether, in fact, they deserve more protection than gunshots or other sounds that don't embody that kind of communication.

MR. ERICKSON: Thank you very much. But let me step a little bit toward the gap there between the two. In the Netherlands, there have been several systems installed in cities that record such things as cries for help. Now, that is speech, certainly, but it is a specific type of speech. Is that –

MR. SLOBOGIN: Well, clearly there is no expectation of privacy there. If you're crying for help, you want everyone to know it.

MR. ERICKSON: And how –

MR. SLOBOGIN: So, I don't think there's any problem there.

MR. ERICKSON: Let me try to push the envelope a little further. They also record sounds that give an indication of fights beginning to initiate. Now, two guys outside a bar are not trying to make public attention to themselves, they are arguing with each other, and it might be predicted to be a fight. In the Netherlands, that's used to send in a patrol officer to try and prevent –

MR. SLOBOGIN: Yes, that's an interesting situation. My guess is there wouldn't be any problem under the Constitution with recording that kind of sound, either.

MR. ERICKSON: Great. Thank you very much.

MS. LEVIN: All right. We're running very short of time, so questions and then quick answers, please.

MR. ECKENWEILER: Hi. Mark Eckenweiler, enforcement operations, Department of Justice. I do have a question, but I just wanted to respond a little bit to something that Marc Blitz said, and also picks up on Deirdre's commentary about cameras being able to zoom in and read the text on a phone that you're text-messaging on. My personal view is, that actually is protected by an REP, and I have had people from the field call me, because my office does the review for applications for video surveillance in private space, and I had someone call me with a not-hypothetical about whether or not they could install a camera in a room like this. It was in a fraud investigation, an overhead view, openly-attended meeting, where they would be looking down and seeing what somebody is writing on a pad. My advice was, I think that's over the line, because if there is a difference between what is generally visible within a room or in a park, and what -- there is absolutely no way to -- a person could see you holding a phone from 100 yards away or more; they are not going to be able to see those characters. I think most courts would, in fact, take that view.

But the question I have is -- it, sort of, goes to Chris Slobogin's, I think, suggestion that legislation is really needed here. I wonder whether or not there really is the will to do so. And let me tell you why I would question that.

We talked about government using video in, say, criminal investigations, installing in private space pursuant to the probable cause standard under Torres. We've talked about public space observation by public and private entities. The one thing we haven't talked about, which, in some ways, is one of the most outrageous cases, is private invasions. And this is something that's come up repeatedly in the last10 or 15 years, cameras installed by the perverted coach in the girls' locker room, by the dad in the bathroom when the daughter's friends come over --there are all dressing rooms -- there are all sorts of scenarios. Every couple of years there is some news story --6 or 7 years ago, it was all these up-skirt photos. It's something I've followed, because from time to time there are proposals for legislation on this at the Federal level. Those have always failed, they have never gone anywhere. At the State level, the reason there's outrage over these dressing-room cases is, it is an astonishing lack in State, many times, if there is any criminal law at all, these are simply misdemeanors. So, the States, I think, have not acted, in the cases that I consider possibly some of the most egregious conduct, to criminally proscribe that. At most, there is a tort remedy. So, given that, I ask you, do you really think that there is going to be a lot of legislative support to address generalized public surveillance, where the issues are so difficult and so hard to articulate in statute what the distinction should be, what the approval should be, when they should be required to be had?

MR. SLOBOGIN: Do I think there will be legislation? Probably not. But on your descriptive point, there are actually a number of States that criminalize the kind of conduct you were talking about. I think there are 12 or 14, at last count. It probably depends, in part, on whether there's been a conspicuous event that's led to the need for legislative reaction.

One of the reasons I think courts should be involved in this whole process is so they can nudge legislatures toward taking some steps to regulate closed circuit TV. For instance, I think if the Supreme Court hadn't decided Berger and Katz, Title III probably wouldn't have come to fruition as quickly as it did. So, I think it's useful to have courts involved.

I think meetings like this suggest that a large number of people, even those who love CCTV, still think there ought to be some very detailed regulation of it. I think one of the best ways of accomplishing that is to get a legislative delegation of regulatory power to the appropriate authority to come up with the policies. One last case I want to mention is the Wells case, a Supreme Court case which made it very clear – granted in the car inventory context, a context that's different from this one -- but nonetheless made it very clear that the Fourth Amendment can be violated if the relevant executive agency engaged in the investigative action does not have a written policy. Without a written policy, in other words, it's per se a violation of the Fourth Amendment.

MS. MULLIGAN: I think that, for a bunch of reasons, we're not going to get Federal legislation anytime soon. I think you're right, there are actually a lot of States -- I think it's closer to 30 – that have the up-skirt/down-skirt, I can give you a list, if you want. There's a lot. Most of them are poor, as you said. And, in part, because it's stuff that you wouldn't be able to see unless you used a camera in a tricky way. It's very hard -- and my husband's a photographer -- "Don't use the telephoto lens, honey." What do these statutes mean?

But I -- for a normative reason, I actually think that there is some value in not having legislation right now, and that is because I think much of what we're looking to do is -- yes, I want police to be able to use all different kinds of technology in ways that make sense. I don't want them to have their hands tied as the criminals go off and be the early adapters that they are. Right, Marc? But I think that, in many ways, getting in and talking with police departments, which is what we've been doing and talking with them about how they see this technology advancing their policing mission, and what kinds of concerns they have about internal abuse, internal misuse, external, what are the issues? And crafting policies from the bottom up are a better way to effect what I would call, kind of, a culture change. It's another reason why I think the process tools, like the privacy impact assessments, are really important, and because they get people, who otherwise wouldn't be thinking about these issues, engaged with the issues and thinking about the ways to tailor the technology or to create the policies.

So, I think that we will have legislation, eventually. You could have a worst-case scenario, where we have the kind of legislative activity you've seen on RFID, where some people want to ban the technology. You can never have an RFID bracelet on the Alzheimer's patient, right? That can't be right, right? And so, I think that there's a risk that, if people don't develop rules, and we don't see bottom-up development of policies, we'll get legislation, and it won't be stuff you like, right? Now nobody's going to like it. And so, I think there's always a sweet spot between policy development and, kind of, the timing of legislative responses. But, I think, at the end of the day, we will have a legislative framework that creates rights and remedies. But I think a lot of it will be process-based, because I think we've all talked about the contextual nature of whether or not different kinds of cameras are okay to use in different kinds of contexts.

I've told people who have asked me about whether or not they can read people's messages that they shouldn't do that, too.

MS. LEVIN: Okay.

MR. WALKER: Seth Walker, City of Columbus, Department of Public Safety. As we look at privacy made up of all these other rights in this penumbra of rights, I'm starting to see, in legal research and strictly in dicta or in papers that are being put out from local law schools, this idea of a right of anonymity, which I know several of the panel members have touched on, not wanting to know -- haven't known whether an individual is going to, you know, an

AA meeting or an abortion clinic or what have you. Is it the feeling of the panel that this might be something that, in coming years, develops more fully?

MR. SLOBOGIN: I hope it does develop more fully, apparently contrary to your hopes. But I don't know if it will. If you want more on that particular right, read the book. [Laughter.]

MS. MULLIGAN: Well, I do, people think it's being in a public place and being noticed, but not being known is different than being in a public place and having a camera that's automatically identifying you and telling everybody who you are. I do think that people feel differently. Clive talked about the license-plate recognition technology that can immediately be used to figure out, with some degree of error who's driving -- who's in the car. I think that, both domestically and internationally, the concerns around national identification cards and having to identify yourself -- people, feel, kind of, peculiar --we don't want license-plates for ourselves so we can be automatically recognized. And so, I think some thing is there, but I don't think it's particularly well formulated.

MR. BLITZ: Just real quick. As you already know, there probably -- there already is a right to anonymous speech, under the First Amendment, that prevents the government from forcing you to disclose your identity in certain circumstances. And one interesting question, although I don't think we're nearly there yet in CCTV, at least from what I've heard, is how use of CCTV could interact with that First Amendment right to anonymity.

MS. LEVIN: Okay. Dave?

MR. D'ANGELES: Hi. Dave D'Angeles, with the Department of Homeland Security. Was a little not too happy with it just being generalized for general law. And a couple of comments on that.

In the surveillance detection courses they teach, that they do multiple surveillances, they do dry runs, they train, they do everything like that. In your research, have you considered going to the facilities -- there's a lot of critical infrastructure facilities that have this -- and hear that side of the story instead of just saying it's Joe Cop on the beat that's walking around, and it's protecting stores and looking at critical infrastructure? One example is there was a facility in the Northeast that, prior to getting their cameras, had 212 cases of potential surveillance detection in 1 year. When cameras were installed, instead of having the local cop drive 10 miles to the facility, they both would get on the cameras and view it and see that it was someone changing a car, and it cut down. And that's the kind of cost-benefit analysis, I think, that you really need to look at.

Also, the gentleman from Clovis here, the chief of police, and -- have you talked to them about having the cameras in the town, in what's been said over and over again -- the safe areas, that it actually gives them a chance to work in other areas where they're more concerned? And I think that hasn't been paid attention to in these discussions.

MR. CATE: I think these are fabulous points. And, in fact, I disagree with you on the paying attention to. I think that's exactly what we're calling for. You've just articulated a key point of the recommendations that I think we've all spoken towards, which is, when rolling out these systems before investing in them, it's critical to make these types of analytical choices. You know, what will this allow us to do? What are the costs? What are the benefits? I think you've done a great job helping to highlight that it's going to be broad on both directions. So, there may be all sorts of unanticipated benefits, like there may be unanticipated costs. It's that type of analysis, though, that 70percent of jurisdictions using cameras without policies suggests maybe they haven't gone through. And so, for those who have, that's terrific. I mean, that's wonderful. That's exactly what I think's desirable.

MR. D'ANGELES: Also, one -- just one last thing. And this -- again, it's just not clear, out here, what you're trying to say; in particular, from Indiana. You were saying, about saving the data was of no value. That's pretty much how it came across. People were shaking their heads. There's many, many cases, especially in mass transit systems, where, because people have called in to the police, and they've gone back and looked, they said, hey, we were there at about noontime, they've actually looked and seen them doing dry runs, dropping materials, seeing how everyone responds, having people walk over, just that were benign chemicals, but they could have been something that was like Japan. And that's where I think you've really got to look at your mindset and look at the past recordings.

MR. CATE: Well, again, just to clarify, of course, I didn't say that saving the data was of no use. What I said is, you need to be specific about why you're using the camera. For some uses, you need realtime access to the data, you need to know, at that moment, what's happening. Saving it almost always has some use, because it has research value. But, generally speaking, in those system, saving the data doesn't have much use. If the reason you have the system is to collect data for other purposes -- for prosecutions, for whatever -- that may be very valuable. But your example of Japan is, of course, exactly what would worry me. If we're trying to catch someone as they drop the chemical on the subway track, my guess is, a month later is going to be too late. So, for that use in that system, we would need to know that the data are actually being used. And those are the types of questions I think a good policy framework would ask in advance.

MS. MULLIGAN: I would just say, I am always eager to come and meet with people who are in the law enforcement side. I'm not shy about it. I like to learn about technology. I'm really interested in police practices. If that's an invitation, I'm there.

MR. D'ANGELES: I'll give you some people to talk to.

MS. LEVIN: And I do think -- I know Deirdre and Constitution Project have been talking with, and have worked with, a number of police departments, and one of the reasons we asked Bob Keyes, from Clovis, to come is because they really do have a very defined program; they're not one of these folks out there that set up cameras without giving it a great

deal of thought, and with a number of policies wrapped around the program. And that really was the model.

So, I want to thank our panelists. I think they did a terrific job. I ended up with lots of questions I never got to, but that's okay. There's room for more discussion. And please give them a round of applause. And we'll take a 10-minute break.

[Applause.]

MS. LEVIN: I'm going not shorten it to 10 minutes.

[Recess.]