Homeland Security

Department of Homeland Security
Data Privacy and Integrity Advisory Committee

OFFICIAL MEETING MINUTES

Wednesday, June 7, 2006
Clift
Rita and Ava Rooms
495 Geary Street
San Francisco, CA 94102

MORNING SESSION

MS. RICHARDS: My name is Becky Richards. I'm the Executive Director of the DHS Data Privacy and Integrity Advisory Committee. And we're going to start this meeting.

I'd like to start with a few administrative announcements. If you have your cell phone on, could you please turn it off or put it to vibrate?

There are materials outside, if you haven't already received those. The toilets are outside and to the right.

And, finally, we've added a public comment section. It's three minutes at this point. And what we're going to do is we've had quite a few people interested in speaking, so if you could please sign up with Lane, who's at the back of the room, before eleven o'clock, we'll then try and figure out how best to accommodate anybody who's interested in speaking. So if you can see Lane and give him your name, we'll go from there.

And with that we'll give it over to Howard and Lisa.

MR. BEALES: Thank you very much, Becky.

We have a full day I think that I, for one, am certainly looking forward to, to hearing about, a variety of issues on surveillance in public places, and RFID, and other topics as well.

We have a change in the Agenda from what is, if you have the printed Agenda that was available, because Maureen Cooney is temporarily unavailable. It's time to have office crises on the East Coast at this point, and she is dutifully dealing with one. And she will be with us a little bit later. So we're going to go directly to our second speaker.

Our second speaker was to be Matt Bettenhausen, the Director of the California Office of Homeland Security. He was called to a cabinet meeting this morning. And so we have with us his Deputy, Robert Samaan. He is the Deputy Director for Federal Affairs in the California Governor's Office of Homeland Security.

Before that he worked for the Director of State and Territorial Coordination in the Office of Secretary Ridge in the Department of Homeland Security where he assisted the Director in coordination of policy and relations with state and territorial governors.

He holds a B.A. in political science from Lee University in Tennessee and a Master's Degree in political management from George Washington University. Robert has certainly this issue from both sides of the fence. And we look forward to your comments. Thank you for being with us today.

REMARKS FROM THE CALIFORNIA OFFICE OF HOMELAND SECURITY;
DEPUTY DIRECTOR; ROBERT SAMAAN

MR. SAMAAN: Well, thank you, thank you very much for having us, "us" being the Office of Homeland Security. Our Director sends his regards, regrets, and me. So I apologize for the change, but hopefully we'll have a good discussion today. And anything I can't answer I'll certainly bring back and submit back to the Committee.

I also bring greetings from the Governor's Office, and from the Governor who reminded me to make sure that everybody knew that it was time to spend a lot of money while you're in California and take in the scenery while here in San Francisco.

If I may brag for a minute, I think that California is truly ahead of the curve when it comes to our first responders' preparedness and our public safety officials. They've seen it all and are truly ahead of the curve in managing disasters and preventing attacks.

Sharing information and best practices, developing standards and plans, as well as coming together for a common purpose is the best way to prevent a terrorist attack and as well as respond to any emergency, whether it's manmade or natural, all hazards.

However, with sharing information comes a responsibility as a citizen of the United States, a citizen of the State of California, to keep people's privacy and information of the utmost importance to us.

California's mission in Homeland Security matches the national strategy for Homeland Security. We work to prevent terrorist attacks within California as well as the United States, reduce California's vulnerability to terrorism and minimize the damage and recover from any attacks that may occur.

We do this through a multi-layered approach, and our office has six core functions. And, if I may, I just wanted to briefly touch on each of those functions.

Information analysis and warning:

Protecting critical infrastructure and key assets as well as defending against catastrophic threats;

Training and exercises;

Strategic planning; Grant funding and administration; as well as citizen preparedness.

I'm going to go back to information analysis and warning. I just want to touch on those other areas first to give you a better idea of how we work in California to prevent terrorist attacks.

For protecting critical infrastructure and key resources, our Deputy Director, Erroll Southers, a former FBI agent, former LAPD, wealth of knowledge in the field of critical infrastructure protection, he works to make sure that our key facilities are not only documented, that we have those facilities ready if there is a threat, that we are able to notify facilities, make sure that we know where is what, make sure that those business owners have a good relationship with our office and the other public safety officials in California.

Also that comes through the management of the Buffer Zone Protection Grant Program, where we work with local law enforcement and private sector to make sure that key sites have buffer zones around them. Buffer zones could be things such as bollards, fences, extra cameras, things of that nature, to make sure that our facilities aren't vulnerable.

Training and exercises, our training shop works to kind of tally how many first responders in California have been trained. And, of course, I don't have an up-to-date number with me, so I apologize. But they also make sure that when we're purchasing equipment with the grant funding that that equipment goes with training. It's very important that you don't just have the gadgets and the gizmos, but that the first responders understand how to use those gadgets and gizmos and also how to work together in using those gadgets and gizmos.

The exercise part, our Training and Exercise Shop conducts a yearly statewide exercise called "Golden Guardian." Golden Guardian is a statewide exercise that's very much like the federal top-off series. We exercise catastrophic events. We want to stress the system to failure to make sure that we know where our weaknesses and that we can better be prepared for disasters. This year we're adding an earthquake scenario.

So here in San Francisco there will be a catastrophic earthquake that we will exercise as well as a terrorist IED event somewhere in Southern California.

The strategic planning arm of our shop makes sure that the look of those great documents that come out of the Department of Homeland Security and out of Congress are melding well with what we do here in California. We want to make sure that we're integrating into the National Incident Management System which, if I may, was actually based after the California Standardized Emergency Management System. So we've got committees that work on making sure that our systems are compatible: The National Response Plan, the National Preparedness School; the National Planning Scenarios. We want to make sure that we're taking those national models and applying them here.

Grant funding administration, that's pretty straightforward. Our office has received and administered over a billion dollars in Homeland Security grants since 2002.

Citizen preparedness is another very important part of our office. We work really closely with the Office of Emergency Services, as well as the First Lady's Office. The First Lady has taken it upon herself to have a 72-hour campaign to make sure that citizens are aware that, you know, you may be on your own for 72 hours. Have enough food, have enough water available, because first responders in those first 72 hours need to be saving lives and not necessarily supporting the, you know, the day-to-day needs that may be there. So the more people that prepare for 72 hours are actually able to free up the first responders to save lives.

So with that, that kind of gives you a general overview of our office. Now I want to go into the information analysis and information fusion.

The State of California has taken many steps to ensure that a person's right to privacy is inherent. There is a lot of confusion within the United States on information sharing and how intelligence is gathered, shared, as well as ultimately used to prevent acts of terrorism and other malicious activities.

I wanted to start by giving you a picture of our information-sharing system here in California. We have a statewide Terrorism Threat Assessment Center, along with four Regional Terrorism Threat Assessment Centers. They mirror the four Federal Court Districts and the four FBI DOJ regions.

We did that because the Joint Terrorism Task Forces already have a well-identified structure; they have relationships with law enforcement at the local and the federal level. It only made sense to integrate those functions.

It is important to note that these Threat Assessment Centers are fusion centers. Their role is to ensure that all information that is collected across federal, state, and local levels is both protected and used to prevent acts of terrorism.

We have integrated, as I mentioned, into this structure that already exists. We want to make sure that -- I lost my spot. The Governor's information-sharing systems are based on years of privacy laws. And I basically wanted to make the point that the Office of Homeland Security, the California Highway Patrol, and the California Department of Justice, when we partnered in this effort, all the same laws have been followed consistently throughout the years. There's nothing new in terms of, you know, ways that we're surveilling, and things of that nature.

And I think that's a very important point that it's important for a state office of Homeland Security to integrate well into the structures that are already in place and to the public's rights that have been governed by the laws in California and the Federal Government for many years.

There is a benefit to sharing this information and diffusing it. I'd like to bring up a few examples. One such example, our Director likes to mention, when he's out discussing information sharing and information fusion, when he was a former federal prosecutor in Illinois, in Chicago, it was about the time that the Oklahoma City bombing occurred.

The Federal Government there in his office had the lead in kind of looking at the flight manifests of going out of the country and making sure that flight manifests going around the country that something didn't seem right, you know, were there people on the "Watch List" that were flying. You know, they wanted to catch this would-be terrorist. They didn't know who did it, but they wanted to catch the person.

At the same time there was a local police officer doing his job patrolling the streets, patrolling the streets saw a loose license plate on a vehicle. The gentleman was speeding; pulled him over, and he cracked the case wide open. He knew from his training, from the information that had been received beforehand, that this didn't seem right, that something didn't seem right. And while the Federal Government was working all of their channels, it was actually a local law enforcement official that caught Timothy McVeigh.

A Customs official at the Canadian border caught the would-be "Millennium Bomber." Something didn't seem right to the Customs official. The training -- the reason I bring this up is the training that's received is a result of information that's given.

So we want to make sure that our first responders know what to look for when they're doing their daily jobs. Fusing this information together helps us better identify what's going on. If there's trends across the state, are there trends across the United States, you know, hospital visits. Are there odd hospital visits that are going on, people that aren't credentialed asking weird questions, things of that nature, just to make sure that all of the first responders are aware of what's going on and they can identify easily if there's a trend occurring.

There's many more examples of proper training that actually led to catching not necessarily even terrorists but, you know, would-be criminals that were out to harm our economy, our way of life. It's also important to note that many of the 9-11 hijackers had interaction with local law enforcement prior to the attacks on September 11th. My point in all this that if can fuse together information that is received from one jurisdiction to the other attacks will be prevented. And that's why we do this information fusion.

That being said, we want to make sure that we have a check on our activities in the fusion of information. Another step we have taken to ensure that privacy is taken seriously at the Office of Homeland Security and the State of California is the development of the State Terrorism Threat Advisory Group or the STTAG is what we call it.

The purpose of the STTAG is to provide the Office of Homeland Security and the Department of Justice of California with advice on the development and practices for our State Terrorism Threat Assessment Center and Regional Centers.

As I mentioned before, the development of threat assessment and information sharing, as it relates to Homeland Security, while it's a new and a developing field, the need to engage in this effort -- I can't emphasize it enough -- is tremendous if we are to prevent terrorist attacks.

As I mentioned earlier, OHS, the California Department of Justice, and the California Highway Patrol in conjunction with our federal and local partners have already made great strides in developing an information-sharing and threat-assessment structure. It is important, however, that this effort is undertaken with an eye towards protecting civil liberties and ensuring the current privacy protection laws are being followed. These issues are the main focus of the STTAG's work.

Just to give you a background on what the STTAG -- who makes up the STTAG, the Dean of the McGeorge School of Law, Dean Elizabeth Parker, who is the former general counsel of the Central Intelligence Agency, graciously serves as our chair. As you can imagine, being with the CIA, she brings a wealth of knowledge and will continue to prove a great benefit to the STTAG. Other members include -- we've got representation from various community groups: The Simon Wiesenthal Center; other public safety officials, fire, police. We want to make sure everyone's in the same room and going over what we're doing to make sure that everyone is in compliance.

So I guess to wrap it up, privacy is of the utmost importance to our office and other officials around California and the United States. We want to be sure that as we move forward with investigations, as well as information fusion, that we don't forget that truth. I thank you for the opportunity to be with you today, and I welcome your questions.

MR. BEALES: Well, thank you very much.

And I think Mr. Bettenhausen sent a very able replacement, and we're glad to have you.

MR. SAMAAN: Thank you.

MR. BEALES: Are there questions from the Committee? Lisa Sotto.

MS. SOTTO: Thank you.

Thank you very much for joining us.

MR. SAMAAN: Thank you.

MS. SOTTO: We appreciate it, especially the last-minute replacement.

Could you talk a little bit about how you tap in to federal databases? Do you tap in directly, or do you download data? And who has access -- presumably there is limited access. And if there is, indeed, limited access, how is access controlled?

MR. SAMAAN: Sure.

MS. SOTTO: Thank you.

MR. SAMAAN: Well, I guess there's different -- I think a problem that we face at the state level -- and the Federal Government faces, quite frankly -- is that there are multiple ways to get information. The DHS Operation Center, the National Operations Center -- they changed the name from DHS to the National Operations Center, so we're trying to keep track of all the name changes -- but their job is to make sure that that information gets fused and that it comes to us, state officials and local officials, in a coordinated manner. That information is protected. Much of it is "For Official Use Only" labeled, which means that only officials with a need to know may have access to that information.

Much of it is law-enforcement sensitive, which basically means that if you're not a law enforcement entity, you should not be receiving this document. It goes all the way up to "Classified."

Most of the information that we get in the state is of the lower classification level. But DHS does a pretty good job of getting us the information we need. We have ways to communicate securely, whether that's video teleconferencing, phones, secure phones, secure fax, things of that nature. That's one method.

The FBI has their information-sharing systems. The Department of Homeland Security -- I'm sorry -- web-based information sharing systems. The Department of Homeland Security has the Homeland Security Information Network. I wouldn't call it a database. I would call it a collaborative tool. It's more of a real-time. You know they will post events of the day that have gone on. You know, your morning briefs are in there, you know, what went on over the last day and the last 24 hours, things of that nature.

If there's an incident, you can open up a collaborative tool between DHS and pretty much anybody else in that same realm to talk about incidents and to post information and share real-time information.

In terms of databases, we have not established any new databases in California. We were very careful to merge into the existing structures that were in place. It doesn't mean that we won't improve upon those structures. That's the point of having the fusion centers, is making sure that, you know, for instance the Coast Guard's information; the San Francisco Police Department, you know, if they have information which -- San Diego Police Department, San Diego Fire.

We want to make sure that everybody is getting the same information, so we want to make sure that all that is fused. So, anyway, I guess the bottom line is the disparate databases are solved by these fusion centers. And, you know, general stuff such as name checks, you know, back to the national watch lists, things of that nature, stuff that your local law enforcement normally would be conducting.

Does that answer your question? Sorry for the roundabout.

MR. ALHADEFF: I'm Joe Alhadeff. Thank you.

I guess it's -- one is a partial follow-up to Lisa's question and then the other one is a separate question.

The partial follow-up to Lisa's question was: As you're fusing the information in the data center, information comes with different classifications, as you mentioned, --

MR. SAMAAN: Um-hum.

MR. ALHADEFF: -- and people have different privileges related to that information, so is there a centralized way of managing the privileges so that as you fuse the information it doesn't lose its character of use restriction because it's now been fused so that you're actually managing what had been silent information in a comprehensive fashion but with the appropriate access limitations, is the first question.

And the second on was: You were talking about the training exercises that you run, which sounded both useful and fairly extensive. And I was wondering if those training exercises related or had any part of them that addressed security and privacy implications of how you use information, how you gather information, and whether any of them had touched on plans in the future for how information may be limited in something like a pandemic preparedness plan.

MR. SAMAAN: Well, thanks, Joe.

I guess to answer your first question, the fusion of information in our State Terrorism Threat Assessment Centers, our regional centers, people have kind of a uniform level of clearances. And what we're trying to do, and we're working with DHS on this and the FBI making sure that all of our analysts have the same level of classification, you know, the highest level possible. That way they are able to share information without changing the nature of the info. (Maureen Cooney enters the room at 8:56 a.m.)

MR. SAMAAN: Now there's these things called "Tear lines" that DHS and FBI will send out to us. Basically it's -- for instance, they would take a classified document, take out maybe the identifiers of, you know, where they got it. Maybe some names they would take out. But the general picture of what the threat is would come to us in a "For Official Use Only" manner. That way you're consistent and you're not changing the nature of the information. That tear line does happen at the federal level. And we actually prefer that, if at all possible, the information be at the For Official Use Only level, because it is easier to share with public safety officials where it's needed. It doesn't do us much good to have a classified document that I can't share with someone that doesn't have a security clearance.

So DHS manages our security clearances in our office. FBI manages some of the security clearance as well in the fusion centers. So we're trying to keep kind of a level of security across the board to ensure that, you know, extra hoops don't have to be jumped through when we have to get the information out.

I mean part of it is, you know, we all may be sitting at a table together as part of the State Fusion Center and, you know, you're telling me something that happened in San Diego yesterday. And that sounds odd to me because up in Sacramento the same thing happened. You know what I mean? So I think that the levels of clearances doesn't change the nature of the information, if that answers your question. Secondly, in terms of our statewide exercise, yes, we do practice. We start with kind of a concept, a planning conference, if you will, work up to a tabletop exercise. A tabletop exercise generally has -- we do them in different levels, actually. We'll do them at the local level. We'll do them at the state executive level, the Governor's level. It's really the Governor's exercise. He wants to make sure that his first responders and his public safety agencies are prepared.

In terms of data sharing, yes, that is part of the scenarios. So say we're sitting here at a tabletop exercise. You know, it'll come up on the screen and say that information has been gathered, and it'll probably say that it came from -- "This is for official use only" -- it came from the Department -- you know, who originated it, if it was the Department of Homeland Security or FBI.

You may get a generic, you know: We don't know for sure but, you know, there may be a chemical attack in Northern California, just as an example. You know, the source of the information is maybe classified, but DHS deems this a credible, credible threat. That information -- of course, the people around the table are at that level of "For Official Use Only." They're able to gather that information and then make their decisions according to that information.

If it's a chemical threat, is it a, for instance, a threat against maybe chemical facilities. So they would look to see where the chemical facilities are and, you know, make contacts, reach out. So that is the part of the process. Making sure that the data is secure is actually a part of what we do. I mean every person that has access to that information is subject to the disclaimer that says, you know, that this information is for official use only. I mean that is a federal classification. And there are penalties for sharing that information outside of a "need to know."

Do does that answer your question?

MR. ALHADEFF: Yeah. I mean I guess what I was looking for is, is there a module in that training which doesn't talk about information sharing per se but has a -- kind of highlights the concepts of privacy and how they are to be applied in situations.

MR. SAMAAN: Right. Yeah, actually if you're talking more about training and less about the exercises, our first responders go through -- basically mostly -- and I'll look at this from a law enforcement perspective, because I think that that's more where this is geared towards.

California has the POST, which is the Peace Officers Standards Training. They are basically a group that make sure that not only are privacy rights included in a police officer's training but everything else that would go into a police officer's training, law enforcement official's training.

We've also got in California the Terrorism Liaison Officer Program. What that is -- and it's done through POST. And mind you again, you know, these are 28 C.F.R.-compliant law enforcement officers that have been trained in the right to privacy and privacy protection and making sure that they can't just, you know, go and do the things they please if a person's privacy is at risk.

So this Terrorism Liaison Officer Program trains police officers. We would like to do it at every police agency in California, not only to be vigilant and know what to look for, but also it does include protection of privacy.

MR. BEALES: Thank you very much. I think we have used about as much time as we can allot.

We can do five more minutes? Excellent. Okay. Then John Sabo.

MR. SABO: Well, that's quite a button.

I had a couple of questions. I had done a lot of work on information-sharing systems, so it's sort of a specialty focus area. And a question for you, generally information sharing doesn't address personal information when you're dealing with general threats, and so on.

MR. SAMAAN: That's correct.

MR. SABO: But there are instances where currently and we expect in pandemic reaction and planning and situations where you'll be dealing with very sensitive personal information.

My question is: Where -- and you mentioned the Homeland Security Information Network and there are other interfaces between state systems and federal systems.

MR. SAMAAN: Correct.

MR. SABO: And my question is: What steps has the state taken to work with DHS to implement MOUs that spell out not just the technical interface requirements for system-to-system exchanges, but also spell out specific privacy requirements and security requirements on both sides of that interface.

In other words, does California, in your MOUs with the Federal Government, require the Federal Government to adhere to certain sets of privacy controls, not just data confidentiality, but things like redisclosure of data inappropriately or data minimization, that type of thing. And, if so, can you provide some of that information to the Committee in terms of the details of the privacy agreement you have with the Federal Government?

MR. SAMAAN: Sure. Using the Homeland Security Information Network -- and I'll just use that one as an example. As you mentioned, there are many. Kind of a side note, what we're trying to do in California, we've got our own web portal called Cal JRIES, which basically -- you know, I've been talking a lot about fusions, my favorite word of the day, but it fuses together the information from a lot of these disparate information-sharing systems. So it mirrors Homeland Security Information Network, but it also includes additional info for our California first responders.

But to get to your question, the Homeland Security Information Network actually operates on a concept of operations that you must agree to. I don't know for sure that we've signed an MOU per se, and I can actually get back to you on that. But I do know that we are regulated by a concept of operations. Within that concept of operations are those controls. And I can probably provide that to you. I'll have to check when I get back. But, you know, within the Con Ops are how are you supposed to information share. What are the rules of the road here? You know, making sure that personal identifiers aren't included in just, you know, even your day-to-day emails.

You know, a lot of the information that's put into those portals does not include the personal identifiers, as you mentioned. But, you know, they make sure in the Con Ops that they put that in there that, you know, you are not to do that. So I wouldn't say it's an MOU per se, but it is a concept of operations that we have to abide by in order to be able to use it.

MR. SABO: Well, just a quick follow-up. Would you -- do you do audits? In other words, you're also sending data, I presume, or will send information to DHS.

MR. SAMAAN: Um-hum.

MR. SABO: So, likewise, do you have a document -- a Con Ops is more of an operational document; it's not necessarily are governing legally- --

MR. SAMAAN: Right.

MR. SABO: -- binding document.

MR. SAMAAN: Correct.

MR. SABO: But do you have audit requirements on DHS for California data that flows in to them and do you have any plans to audit?

MR. SAMAAN: That I don't know, to tell you the truth. You know, our lawyers in our office actually handle a lot of that information. And I could get back to you on that.

In terms of the way that we share information in California, yes, we actually do have a MOU that we've signed between California Highway Patrol, California Department of Justice, our office. And we make sure that new analysts coming in have to abide by the rules that we've laid out. But I'll have to get that back to you because that's really not my lane.

MR. BEALES: All right. Thank you very much.

MR. SAMAAN: Thank you.

MR. BEALES: We appreciate your time and your information. You've been most informative.

MR. SAMAAN: Thank you for having me. And, again, I'll look forward to -- I'll be here all day. So if you all have questions throughout the day, let me know, and I'll --

MR. BEALES: We'll pick on you.

MR. SAMAAN: -- provide the Chair with my contact info if you want to follow up on anything.

MR. BEALES: Thank you. Thank you.

As we turn to Maureen and get rearranged here, I wanted to note that I found this book on my desk this morning called Identity Crisis, and it had Jim Harper's name on it. And I thought I'd ask Jim to say a word about what it was and whether there were any strings attached.

MR. HARPER: Yeah, the strings are you have to read it.

Thank you, Howard.

I did want to just take a brief moment to present my book to my colleagues. Identity Crisis came out a couple weeks ago. Two years ago or so I recognized that a formal national ID system might be in the offing for the United States. And I determined that I should try to articulate better than I've heard before why we should be concerned about a national ID.

So I began researching for this book, and I found, most interestingly to me, that there was a lack of theoretical explanation for identification. What it is, is a social and economic process, and how it works, for example, in the card or token context.

So more, more than I expected the book is about the theory of identification, how it works, what it works for, and what it doesn't work for. It also addresses why we should be concerned about a national ID, which was my original goal.

And, finally, it finally gets into how we can get the benefits of identification, it's an absolutely necessary process, while minimizing the concerns about surveillance and tracking, and that kind of thing. So in closing I want to read my favorite blurb from the back. It says:

"Identity Crisis does the best job I've seen of addressing the real weaknesses in current identification systems and how they correlate directly with further impingements on our privacy and civil liberties. I would have used this book every day to help structure programs and develop policies if I'd had it at TSA." That's by Justin Oberman, --(Laughter.)

MR. HARPER: -- the former head of identity and credentialing programs at TSA.

So either I've gotten it right or I've gotten it wildly wrong. (Laughter.)

MR. HARPER: Thank you very much, Howard.

MR. BEALES: Thanks, Jim. It certainly sounds central to our work, and I look forward to it.

Our next speaker is Maureen Cooney, who is the Acting Chief Privacy Officer of the Department of Homeland Security. Before that she was the Chief of Staff and the Director of International Privacy Policy for the Department. Before that she was at the Federal Trade Commission doing really important work. And, Maureen, as always, it's a pleasure to have you. And we look forward to the Privacy Office Update.

DHS PRIVACY OFFICE UPDATE, MS. MAUREEN COONEY, ACTING CHIEF PRIVACY OFFICER AND CHIEF FOIA OFFICER, DEPARTMENT OF HOMELAND SECURITY

MS. COONEY: Thank you, Howard.

I'd really like to begin by thanking you, Howard, and you, Lisa, on behalf of the entire Department for your leadership of this Committee, which is so important to the Department.

Someone asked me yesterday: Was there a statutory mandate at DHS to have this Privacy Advisory Committee. And I said, "No," the answer was no to that. We just felt, from a departmental perspective, that privacy was so important that certainly this was very important to be a stand-alone committee to advise the Secretary and the Privacy Office. And so I thank you for your leadership and I thank all of the Committee members on behalf of the Department. We really do appreciate all of your hard work.

I'm pleased to be with you today to give you an update on what we've been working on in the last quarter since we all last met. And I guess I'd want to begin and underline what the primary mission of the Privacy Office is and certainly what I see my commitment in this role being, which is to fully integrate privacy considerations and compliance into the way in which we carry out our security mission at the Department.

I think that that's what Section 222 of the Homeland Security Act really requires of us as a Department to integrate privacy into the way we carry out our security mission. And we try very hard to do that, but not in a vacuum. We absolutely depend on partnerships throughout the Department and on leveraging staff resources and good ideas from all across the Department.

So I would want you to know I would commend to you the terrific staff of the Privacy Office and I'm so thrilled to be a part of such a good group. But I also want you to know we really rely on strong partnerships across the office with the CIO's Shop, with the Law Department, with the Policy Shop and, of course, all of our operational programs.

To fully describe how we try to operationalize privacy in the way we push out programs from the Privacy Office, I think I would recommend to you some of the testimony that we recently gave to Congress in this last quarter.

I had the opportunity to testify three times on behalf of the Department. The first was on April 4th, and that was before the House Judiciary Subcommittee on Commercial and Administrative Law jointly with the Subcommittee on the Constitution.

That particular testimony -- and I believe that you, as well as the public, have copies of our testimony -- addressed how the Department tries to be transparent and attentive to the way in which we use commercial data that we take in from data aggregators. I think what that testimony will point out is the beginning of efforts, not the end of what we're doing at DHS.

We are working very closely with operational groups within the Department, a cross-sectional committee, to come out with privacy guidance just to that particular subject in a way that will meld well with the way operations are carried out.

So to be attentive, to make sure we're not getting in the way of carrying out our security mission, but also making sure that across the board in the Department we have a harmonized approach, and we're working very actively on that.

On April 6th I testified before the House Homeland Security Subcommittee on Intelligence, Information Sharing, and Risk Assessments. And the topic for that particular testimony was how we integrate privacy into the DHS intelligence enterprise.

Charlie Allen, who heads up that particular area and is, of course, over the Intelligence and Information Analysis Group at DHS has done some follow-up testimony before the same Subcommittee on the same topic.

On that particular testimony I think it may be one of the better examples, I hope, for fully describing all of the different touch points where the Privacy Office is active in integrating privacy considerations into our programs, including our national intelligence programs and databases.

We have a very strong partnership with our information and analysis units. And we're thrilled with that. We hope that it will, perhaps, be a model for others in the intelligence community. On that I might note, while that testimony didn't fully discuss it, we work very closely with an Information Sharing Environment Board -- and I think I mentioned this a little bit at the last testimony -- we've worked very closely in developing procedures to carry out Guideline 5 for the information-sharing environment, which is on privacy. It's not finalized yet, but I think it will soon be finalized across the Federal Government and be shared for comment.

Finally, we testified on May 7th, again, before the House Judiciary Subcommittee on Commercial and Administrative Law. It was an oversight hearing on privacy in the hands of the Federal Government. That was the title. But the focus really was on the role of a chief privacy officer within a federal agency. And it gave us an opportunity again to talk about how we're trying to operationalize routine processes at the Department of Homeland Security in being privacy attentive.

We particularly focused on our privacy impact assessment process, but as all of the different testimonies point out, that's not our only means. It's just one touch point among many across the lifecycle development of technologies and the development of programs and roll-outs. I'd be happy to answer any questions on that.

Other activities within the Privacy Office that I would bring your attention to, and I understand that some reports may not have been delivered physically to you, but we'll get them to you, a report that we were required to do by Congress on assessing the impact to the automatic selectee in no-fly lists, it was required under Section 4012(B2) of the Intelligence Reform and Terrorism Prevention Act.

We sent that to Congress in April. It was a long process of writing and iterative process across agencies, many of which touch the use of the no-fly and automatic selectee lists. We found in our report several things. And one of the things that we were asked by Congress to look at was the appropriateness of using these lists for broader purposes other than aviation security.

And our conclusion on that was that, without looking at certain of the legal aspects on being required to use the list, that if they were used more broadly we would need to actually look very carefully at the each of those programs. There were no prototypes for that right now and no considerations of such programs.

What we stressed was that there needed to be a caution about using the lists more broadly because they really are set up right now to achieve a specific purpose. We did find that there were improvements in the list, while more improvements can be made. The Terrorist Screening Center, the TSC, had done an admirable job of redefining the criteria for names being added to the list and for, frankly, cleaning up the list, improving data integrity.

And we also talked about redress and the importance of a strong redress program. And at the Department of Homeland Security that is a continuing issue of both concern and interest to us. I think that we are working very hard with others to look at ideas about a centralized redress and also communicating to the public that DHS alone is not always able to solve consumer or traveler problems because it's an integrated system and we may not have been the original parties to put a name on a no-fly list. So it's really working with others, checking the data integrity. And the TSC plays a central role in being the liaison with the different agencies who actually were the initiators of putting a name on a list and then checking whether that was accurate and should still be there.

Another important report that we were required to do by Congress is a report on data-mining activities at the Department. Our office has completed that report. It is in the clearance process, and we hope to see that shortly released.

Finally, if I may just bend your ear just for a few more minutes. We do have a busy program of outreach from the Privacy Office as well. On April 5th we did a public workshop on transparency and accountability, the use of personal information in government.

That specifically was directed to the use of privacy notices, what they are now, how they can be improved, how they're used in government, and what we can learn from the private sector as well. And it also focused on the Freedom of Information Act which, as you know, the Privacy Office at DHS also has responsibility for freedom of information compliance and policy.

It was an excellent opportunity and workshop to hear views from the public. It also was a wonderful opportunity, from my vantage point, to have many international visitors there. A group of data protection staff who are part of what is known as "The Berlin Group" -- they're from Europe, all of the member states -- as well as representatives from Japan and Mexico and other countries who attended and participated in that workshop. So it was very good to have that comparative analysis.

Finally, I want to promote a workshop coming up that we're hosting next week on June 15th. And it's called, "Operationalizing Privacy." We'll be looking at compliance frameworks and privacy impact assessments. And we're using it both as an outreach effort and as hands-on training for our own employees at DHS and partnering with the Department of Justice, actually including many of their employees in that training session as well.

The April 5th workshop was sold out, standing room only. We're expecting that same kind of response for this upcoming one. I think our last count was we were nearly at 200 and we hadn't done any real press outreach on it.

And finally, if I may, just speak a little bit to international efforts. We continue to outreach to our international partners, both in a learning mode and in a communicating mode. Most recently we participated last week in a U.S. Government outreach where we gave presentations to our State Department, Department of Justice, and DHS employees who are abroad in Europe so that they fully understand privacy laws and frameworks in the United States and can communicate those.

And a couple of months before that we did a major presentation at the First European Congress on Data Protection in Spain. And our focus there was an identity theft discussion.

There is no more urgent matter I think in the Federal Government right now than looking at data security and how that impacts identity theft certainly since the announcement of the Veterans Administration breach. And we're very attentive. We have been. We have had ongoing projects at DHS prior to that.

Since the announcement of that breach, certainly our office has been active within the Department. And two weeks ago we wrote guidance for our employees on that issue. And we're working very closely with the CIO Shop and others throughout the Department in getting those messages out to employees on how to responsibly handle information that really is a public trust in our positions at DHS.

Thank you for this opportunity. And thank you again for your service and advice to the Department.

MR. BEALES: Thank you very much, Maureen. I think I speak for all of us when I say we really appreciate the support and the staff support from you and your office for our work. And, you know, we look forward to try and be helpful.

Do we have time for questions? Maybe one question, if there's a question.

Joanne.

MS. McNABB: Maureen, what advice did you give to your employees on the VA breach?

MS. COONEY: We gave a number of touchstone points that we thought that they should follow. Certainly advising them, number one, that we have an active privacy management directorate -- directive within the Department that outlines steps they need to be attentive to so that they have the document and could read through what their roles and responsibilities are.

We asked each of the program managers to make sure that their employees knew what information should and should not be leaving the office. We talked a lot about the use of passwords and encryption of data.

We talked about cleaning disks and how to do that. If you were using information and transporting it and then were finished with it, how that should be attended to. And then there were actually a list of other steps. I think it was fairly comprehensive.

At the same time I would say the directive that we composed also notified employees they would getting more fulsome guidance within about the next hundred days. That is not only a DHS roll-out that will happen, but government-wide. We expect that every agency will be reviewing all of its programs, which we've asked people to do, and finalizing broader guidance on how to deal both with data security and data breach notifications.

MS. McNABB: Thank you.

MR. BEALES: Lisa Sotto.

MS. SOTTO: Thank you. Just a quick follow-up.

I'm just curious as to whether DHS encrypts its laptops and other portable devices.

MS. COONEY: Routinely, yes. And our system requires that. If you were using a system offsite that's encrypted, the data is encrypted. I think what we're looking very closely at is to make sure that all of the systems are the same no matter which type of employee is using it, whether it's a DHS employee or a contractor. Those who have access to our networks and can download information certainly come within that sphere of encrypted information.

MS. SOTTO: Great.

MR. BEALES: Thank you very much, Maureen. We really appreciate your report.

Our next speaker is Charles DeMore. He is the Special Agent in charge of the Immigration and Customs Enforcement Office of Investigation here in San Francisco. He was the First Assistant Director of the newly-formed ICE. That's Immigration and Customs Enforcement Office of Investigations in Washington, D.C. He began his career in INS where he was the Assistant Commissioner for INS Investigations at Headquarters in Washington.

Mr. DeMore, thank you for being with us today.

BORDER MANAGEMENT AND ENFORCEMENT: MR. CHARLES DeMORE, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

MR. DeMORE: Thank you very much.

I hope I can be of some value to you. I'm certainly not a subject-matter expert on privacy, but I certainly am pleased to be able to spend a few minutes talking about what I do and what ICE does.

I was asked to spend 15 or 20 minutes talking to you about two things, really: The evolution of ICE as a component of Homeland Security and then how we are vital to and the nexus we have with border management and border security.

I'll start off by telling you this is a very interesting environment that we work in here in San Francisco. I'm going to talk about two things. The evolution of ICE and the Secretary's role out of SBI, which is the Secure Border Initiative. And, I think instrumental to a discussion of the Secure Border Initiative is knowing where we hope to end up.

SBI is the Secretary's blueprint for really global immigration reform. We talk about border management, it's more than that. It's immigration reform. And what makes this difficult is that you know it's hard to get where you want to go if you don't know when you leave where you expect to get to.

And the Secretary has laid out, I think, a real good plan. I started my career 23 years ago as a Border Patrol Agent, so I have my five years working on the border in an environment that was incredibly chaotic. I mean I used to see just -- in a totally uncontrolled environment. Now I go down and it's incredibly different.

But we need to know where we want to get to. And to underscore how challenging this particular problem is for us, when the Secretary rolled out last month SBI Part 2, which is the interior enforcement component, the article that appeared in the paper here locally was: Mayor vows to defy immigration reform.

So I think as a nation we need to come to some grips in terms of what the immigration, if you want to deem it a problem, what the immigration problem is and then develop a strategy for effectively dealing with that problem. I don't know that we're there yet. I think, as a Department, we're there; as an administration we're there; as an agency we're there. I don't know as a country if we're there.

A few years ago I was speaking to a group of folks here in San Francisco, and one of the things I did was to hold up -- we get from our Public Affairs Office daily news clips that come out. And five years ago, when I read the clips, I said, "Let me just give you an example of how conflicted this country is right now with respect to immigration."

There were all kinds of articles that were pro immigration and anti immigration, but there were articles like, you know, states debate the propriety of issuing drivers' licenses to illegals and schools debate the propriety of allowing, you know, public-subsidized education for people in the country unlawfully.

Now when you read the daily clips they're by and large very pro enforcement. So that that pendulum has swung back significantly. And I think it's very critical for all of us and prudent to ensure that the pendulum stops at the right place, that we have a well thought out, deliberate, constructive immigration reform protocol in process. And I think the Secretary has laid one out.

But first let me tell you a little bit about ICE. I was the District Director for INS here for six -- well, I was with INS here about seven years, and now I've been here with ICE from about three years. I was called back to Washington in 2002 basically to run the Immigration Investigations Program.

And as soon as I got there I found out that the immigration agency was about to be abolished and I was part of a reorganization in the context of Homeland Security. A couple of things that I think led to the demise of the INS had to do with our own internal mission conflicting.

We were an agency that was both a law enforcement agency as well as a deliverer of benefits. We had what they called a dual-management track protocol in INS. That means that, for example, I came up in the Border Patrol, so as I moved up in the management ranks as a law enforcement officer I managed the law enforcement portfolio, but I also managed the delivery of services portfolio.

Conversely, if someone were to have come up on the benefits side, they had never had any law enforcement experience, once they went into the management ranks they were supervising both delivery of benefits and also law enforcement. People saw that as a problem. And law enforcement people supervising benefits and benefits people supervising law enforcement. And then obviously we all know what happened on 9-11.

In the aftermath of 9-11 people started asking very hard questions of the INS. Who do we know that comes into this country -- or how do we know if people who come into this country have left. And we didn't. We had really no viable means to identify who that had come into the country had left and who hadn't left. And that's really an unacceptable situation.

So the beginning of the end for the INS. The beginning of the beginning for DHS. ICE is an amalgam of a number of pieces of what was the Immigration Service. And to kind of break it out -- I don't know if people are familiar with how the immigration piece, you know, what came from what was. The INS was broken up into three different agencies. CIS, Citizenship and Immigration Services basically became the deliverer of the benefits.

CBP, Customs and Border Protection, became the one face at the border. And that merged customs inspections with immigration inspections and agriculture and public health and the Border Patrol. So the idea was just one face at the border.

And then a third and separate agency is ICE, Immigration and Customs Enforcement. And we became -- basically from my program, investigations, we merged immigration and customs investigations and tried to find some synergies in those broad statutory authorities that we could leverage in ways that had never been leveraged before.

And it's been a long and sometimes difficult process creating and living this new agency, but it's been a very -- it's been of great value, I think, to the country that we've merged these agencies and applied our authorities in ways that we had not before.

In terms of this border management issue, and I know I don't have a lot of time, but I think you have to think of the border somewhat as a virtual reality as much as a physical one. We're all familiar with, you know, the land borders, the frontier on the Canadian and Mexican borders. But the border is right here in this room. I mean your laptop computers almost constitute a virtual border because if someone can use that computer to send technology that could be used against us to our enemies abroad they've in a certain sense breached our border.

If they can use that computer to make financial transactions that either move money into or out of this country into the bank accounts of people who would do us harm, we are at a much greater risk. So you've got that kind of cyber world, that kind of cyber border that you have to be cognizant of.

You also have the air border. You know, we do a great deal -- in terms of border management, border management really starts abroad. You have to go overseas and work with host country law enforcement, host country governments to try and effectuate some constructive change there to keep people who would do us harm from getting on an airplane in the first place.

But that being said, you're still reliant upon their people, their technology to safeguard our interests here. So someone who gets off an airplane in San Francisco is, legally speaking, not in the country. They're knocking at the door. Technically they're not here, although they're standing in San Francisco. They're now potentially a threat to us.

And then we have, of course, our seaports. And here in San Francisco, we have Oakland. The Port of Oakland is the fourth largest port in the country. So I would ask you to think very broadly in terms of what constitutes a border.

ICE is composed of three basic operational areas. The first one I'll talk about is financial. That's really at the foundation of what we do. We try and dismantle criminal enterprises by going after the revenues that support them. You know it's one thing to take drug dealers off the street; it's another thing to take away the revenue that supports the institution.

So we do two things in our financial arena. One, we investigate financial crimes: Money laundering and associated crimes; bulk currency; smuggling; the use of hawalas, nontraditional banking systems, that type of thing.

And then we also partner with the financial community, the banking and financial community, to help them identify and mitigate vulnerabilities that are systemic in the institution, in the financial institution. So we're partnering on the one hand; we're investigating and presenting for prosecution on the other.

In our Public Safety Division we have a number of initiatives. One is alien smuggling and human trafficking. Here in San Francisco we just recently -- excuse me -- I say "recently." In the last year we took down an organization that was smuggling Korean females for the purposes of prostitution. It wasn't simply a smuggling operation; it was a trafficking operation. The difference is if you're smuggled, you're somewhat complicit. You make arrangements with a smuggler to be moved from one place to another, from outside the country to inside the country for a fee.

If you're trafficking, it involves the elements of force, fraud, or coercion. You're either snatched off the street, so to speak, or you're intimidated in terms of if you don't do what we want you to do we'll harm your family back in Korea.

We actually arrested 104 Korean women, processed them administratively. And the way we saw this is they were the victims, not the criminals. And we're in the process now of prosecuting a fairly significant number of people, about 35 people here in the Bay Area. So smuggling, trafficking, contraband smuggling. We're involved in everything from genetically-engineered weed seed that could be used to damage our crops to the illegal importation of whales' teeth, anything that crosses that border is of interest to us. So whether it's coming in or going out, if it's coming in and it's contraband it's within our purview.

Criminal gang enforcement, we have a very robust criminal gang, foreign nationals involved in criminal gangs. We've actually arrested 49 people I think in the last week in the Northern California area. My area covers 49 of the 58 California counties, northern Nevada and the State of Utah.

And then IPR, intellectual property right violations. We're very aggressive there. You know, you hear about the typical ones, I mean the phony Rolex that somebody buys down in Mexico for $20. I mean that's one thing. But what we're seeing is much more egregious than that. We're seeing counterfeit products like baby formula. You know, think about your child or your grandchild or your, you know, friend's child ingesting baby formula that's counterfeit. It's a knock-off product.

I mean we've seen extension cords with the URL, Underwriter Lab, you know, label on it, but they're counterfeit. And I always think about, you know, the person that puts the Christmas presents under the tree, plugs the tree in and goes to bed and, you know, God forbid that that product is not going to allow you to, you know, safely operate that. Cigarettes, contraceptives, you know, you name it; we see it.

And then immigration fraud would be last thing in our public safety arena, whether it's employment fraud -- I think when the Secretary rolled out SBI, he's really looking at taking away the magnet, because you cannot control the borders if you're not in control of the interior. If that magnet radiates, it will attract people and they will come. Conversely, if you can't control your borders, your interior is vulnerable. So these things have to be looked at. Border management has to be looked at a complementary synergy between the interior and the physical border itself and, for that matter, the virtual border.

And then our last area is our National Security Unit, where we are -- we're the second largest contributor presently to the Joint Terrorism Task Force and FBI Initiative. I'm sure you're well familiar with it. It tries to protect our national security interests.

And really in the aftermath of 9-11 I was detailed from here to Washington on maybe, I don't know, September 15th or 16th. And there were a lot of people that were identified as having potential national security, that we saw as risks, or the intelligence community saw as risks, or the FBI saw as risks.

And the one element that allowed for those risks to be somewhat neutralized were the administrative authorities under Title 8. We are able to leverage our administrative authorities and use them in ways that no other agency can do. And so that's where the value of that immigration piece has always fit in.

And then the last area under our National Security Unit is our strategic investigations, which are violations of the Arms Export Control Act, people who are exporting things that require a license like night vision technology, laser-guided systems, propulsion technology, that type of thing. So those are really the component pieces of ICE.

And now in terms of SBI -- and tell me if I start to -- three minutes? Okay. SBI, the Secretary identified three strategic goals: Identify and remove incarcerated aliens that pose a threat to the communities, build strong compliance and enforcement programs with employers and uproot criminal infrastructure.

The second bullet is the one that I would be most interested in, and that's building strong compliance enforcement programs with employers. I think the idea that we are going to continue to grow as a country through immigration is a given. It's the right thing to do. It's what we will do, but it has to be done in, as I said before, a constructive and thoughtful manner.

We need -- you know, I'll try and wrap this up real quickly -- it's just ironic that in the Cold War they had a wall that was designed to keep people in, and now there's discussions in this country about building a wall to keep people out.

What it is that cause those people to want to flee or what it is that causes these people to want to come is the opportunity to work here unlawfully. And the Secretary, I think, has very appropriately focused on the need to work with, not to work against, but the need to work with employers to create an environment where people come and work legally. And I don't think it's complicated at all.

And my final kind of comment would be that I've always advocated that we should have a single employment authorizing document, just one. Right now we have Social Security cards; we have employment authorizing documents issued by our agency, by CIS. Have one document, have it constructed by professionals, whether it's, you know, a Visa or MasterCard or whomever, have biometric data, and then over a phased-in period of time have a responsibility that employers have card readers and scan the card and we know that that's your card and you're able to work legally.

I think until we get to a point where we're able to police the interior it's going to make it very difficult for our enforcement people on the border to effectively do their job.

And in closing I just wanted to show you one picture, because I know that you guys are also involved in technology, and so forth. And I just wanted to show you what can happen when ingenuity overcomes technology. This is actually a picture of like a '53 Chevy truck that these people converted to a sea craft by putting a propeller on the drive shaft and then attaching floatation devices, and they were driving it from Miami to -- I'm sorry -- from Cuba to Miami.

So it doesn't necessarily take a whole lot -- and I brought one other picture, just examples of some of the stuff we're seeing -- it doesn't take a whole lot of technology to find this. I mean we have Naval warships and Air Force jets, satellite technology.

But on the back end of finding this, there's an incredible resource draw from the standpoint of the agency, beds, litigators, agents, deportation officers, courts, and that the first thing. So we're spending a whole lot of money. And I think that we all would probably agree there are smarter ways to work.

And I would suggest that the Secretary's Secure Border Initiative is probably a very, very viable and good way to go. I thank you for your time.

MR. BEALES: Thank you, Mr. DeMore. I think we only have time for like one or two questions.

Jim.

MR. HARPER: For the book.

Well, thank you for your presentation.

MR. DeMORE: You're welcome.

MR. HARPER: I appreciate hearing your description. I think a clear one of the direction of the interior enforcement policy, which is to require every American to carry a national ID card in order to get federal approval for working. So I don't need to go into that. You've done it quite well.

I wanted to ask you, though, just briefly about an observation you made about the fact that computers and communications devices represent a virtual border. As many of us know, people enjoy a diminished right to privacy or diminished Fourth Amendment rights at the border. And that's for good reason, I think, in the traditional border context.

But I just want to know if you think that people's computers and communications enjoy less Fourth Amendment protection because they can be used to communicate internationally.

MR. DeMORE: That's a very difficult question and one that I'm not so sure it's appropriate for me as a law enforcement practitioner to weigh in on the policy issues. I mean I leave that for really the experts like yourselves.

I think it's of the utmost importance that we use every tool available to us as law enforcement officers to protect the American public. So that being said, I think people absolutely have a right to privacy. I appreciate my own right to privacy. In addition to being a Homeland Security law enforcement person, I'm an American. I try and balance always the interests of law enforcement with the right of people to be secure and private in their own homes and in their own... so.

MR. BEALES: Ramon.

MR. DeMORE: And, by the way, sir, I have to say I didn't call it a national ID card. I called it a sole employment authorizing document.

MR. BEALES: Thank you, Mr. Orwell. (Laughter.)

MR. BARQUIN: I'd also like to follow up on your virtual border, because I do think it is extremely important. And given that, as you well indicated, this is very, very much an area where we as a country are trying to sort through with all of the thrusts that are happening vis-a-vis outsourcing a lot of the work there may be that there is less of a need for actual immigration if work is being done elsewhere. And that in some cases it's good; in other cases it's bad.

But the focus on this virtual border and the privacy implications, which is what our principal concern are, seem to be an area that ICE is very much in the middle of, so I wanted just to have you comment a little bit on what ICE specifically is doing vis-a-vis privacy and data integrity issues related to this virtual border.

MR. DeMORE: Well, for us, and we're using our investigative authorities working in a cyber arena pretty generically and without, you know, going and looking at anyone who is not generally soliciting us for some kind of criminal activity.

I'll give you a few examples. We have people who will go online and join chat rooms, and they will be solicited by people online to engage in, you know, sexual activities. We're not going out to you and saying: Hey, would you be interested in engaging in this criminal activity? We're going out and letting people approach us.

Similarly, and two quick cases here in the San Francisco area, in the last month we had a Saudi Arabian psychiatrist who, over the course of a year, corresponded with a detective on a task force with our agents who he thought was the father of a three-year-old that he wanted to molest. We didn't go out looking for him. We didn't solicit him. He came to us.

Over the course of a year he agreed to come into the United States to actually molest this child, and he showed up at a Motel 6 in Vallejo about three weeks ago, and now he's sitting in jail.

We also just brought back from Laos -- I'm sorry -- from Cambodia a Bay Area gentleman who was over there molesting children.

But in the cyber arena, you know, in the sex world they're coming to us. We're not, you know, out baiting.

And the other piece is in the strategic arena, we may go online and say: Hey, we're selling laser-guided technology, and people come to us to buy it. We're not going out to you and saying: Hey, we've got the stuff. You know, it's really licensable, but we'll sell it to you anyway. We're just going out saying: We have a product to sell. And then when they contact us, we're saying: Well, you know, this is not for export and if you buy it from us you know you legally can't export. And so then I mean it just starts the thing rolling.

But I think unless you have a criminal intent at least from the standpoint -- and I can only really speak to my office here and how my agents are conducting their investigations -- unless you have a criminal intent and a predisposed, you know, wish to engage in this criminal activity we're not out casting some wide nets to find people and then encourage them to do something they wouldn't otherwise do.

MR. BARQUIN: I just need to comment on your picture of the, as we call them, camino noltas in Spanish, the Cuban in the truck, which was followed shortly after by one of the same individuals in a Chevy that he converted. And I just want to put in a word, because I understand you've got to enforce our immigration laws and I'm sure it's the Coast Guard, but I'd love to have some of these actually kept for a museum later on, because they deserve it, rather than just sunk as they are up to now.

MR. BEALES: I think our last question, Tara.

MS. LEMMEY: Many of the things -- mostly this is a question for the Committee -- many of the things I think we just heard I find somewhat concerning, sort of beyond the level of questions that you're capable of responding to because they're policy and beyond the purview. And what I'd like to make sure we put on the table is for the next meeting perhaps we can ask more speakers to come who can address some of the more specific issues as it relates to identity and policy.

Many of the areas you covered fall more into commerce. And there are things that we might even question on that side, but it's outside of our scope.

I would like to ask a little bit of a question, though. Yesterday we were at SFO looking at some of the exit technologies being considered and opportunities there. And it seems like there's a real leaning towards technology for doing some things that perhaps technology is not best optimized to do.

Have you spent much time on the exit issue and what's your role in that?

MR. DeMORE: No. I mean I don't have a direct role. That's obviously CBP. I've given it a lot of thought because it's obviously a very complicated issue, how you capture that departure data in a meaningful way and not allow, you know, your own enforcement efforts to be undermined or exploited. But I'm aware of some of the various technologies that are out there: RFI and other things. But I'm not personally engaged in that process.

MR. BEALES: If I could just follow up just a little bit. Could you say a few words about why that data is important? I mean what do we gain by capturing better exit data?

MR. DeMORE: Well, if we don't know who departs, we don't know who's here unlawfully. I think it only makes sense that we should have some kind of oversight of the visa issue when it's processed in terms of you get a visa; you're expected to abide by the conditions that predicated the issuance. And the only way to ensure that you are abiding by the conditions are to ensure that you departed timely.

MR. BEALES: Is there any sense of the magnitude of the illegals who are overstayed visas who didn't exit as opposed to the ones who entered illegally in the first place?

MR. DeMORE: Well, the estimates that I've read for a long time are that roughly half of the people that are here unlawfully came with a visa and then overstayed.

MR. BEALES: All right. Thank you very much.

MR. DeMORE: You're welcome.

MR. BEALES: We appreciate your participation today.

MR. DeMORE: Thank you.

MR. BEALES: Our next speaker is Clive Norris. He is the Deputy Director at the Centre for Criminological Research at Sheffield University. He became a lecturer in criminology in 1993 at Hull and began to develop his research profile and his interest in the sociology of surveillance. At present he's working on a comparative study of the social impact of closed-captioned TV in seven European countries.

Mr. Norris, we really look forward to hearing from you today. Thank you for being with us.

CLOSED CIRCUIT TELEVISION: MR. CLIVE NORRIS, SHEFFIELD UNIVERSITY CENTRE FOR CRIMINOLOGICAL RESEARCH

MR. NORRIS: Thank you. And it's a privilege to come and talk to you. I prepared a paper for this group, and I'm basically going to talk loosely through some of the main issues that I see that have arisen over the last 15 years that CCTV has developed in mainly the UK but also drawing on the European experience.

So I'm mostly going to review what we know from the British experience about CCTV in a way that I think matters in terms of privacy.

Let me start by just trying to get some definitions straight in terms of what is CCTV, because I think this actually matters very much if one's considering how to regulate the technology. At its most basic, CCTV is a camera, a cable, and a monitor, not even a video recorder. So that actually is very different, too, when you add a video recorder. But also just adding a video recorder does not actually help very much, if you're talking about mass surveillance systems: One camera, one monitor, one video recorder.

What has happened since the 1960s, and they were the systems that mainly occurred in the '60s in retail shops and in limited environments. We've seen a gradual growth. We've seen four cameras, a monitor. But then how do you display four cameras? So you split the monitor, and you have four images. Then how do you record the images? Do you have four video recorders?

Well, no, actually what you tend to do is either time lapse the tape or multiplex the tape. You take one frame out of 20 or one frame out of four and store sequentially or you split the videotape into four segments so that you don't have so much information. I think that's the important thing. What happens here is, of course, you get information loss as you transfer a system. So CCTV is actually quite complex in the sense that we have in Britain systems that literally are a camera and a monitor with a bit of cable, no recording device.

And then we have systems which are 400 cameras digitally recorded or come on to that. So every camera is recorded in realtime, very little information lost, and so forth. So you're talking about a very wide range of technologies.

Secondly, cameras do nothing. A bit of plastic, some glass, some wires, a monitor. In themselves they actually have no social, criminological, or privacy impact. It is only when we understand them as part of -- as a social -- I call it a social technical system. It's only when people know that they're being watched by a camera and alter their behavior because of it that it starts to take on significance or that somebody else is watching and actually does something on the basis of that knowledge.

And actually that's very problematic. If you look -- if we think we know what CCTV is, what we see across Europe, and I suspect across America, is a vast range of systems. We have CCTV systems, but some of them, for instance, are only watched sporadically. Some of them have people watching the screens day and night.

Some of them have Pan, Tilt, Zoom cameras that can track people as they move across space. Some of them have then a relationship between those who are watching and the law enforcement agency or a private security agency through radio and maybe through video links, which means that they can direct police officers or security officers to a particular incident.

This matters in terms of how you understand it. In the study I carried out some years ago we looked at three control rooms, spent 200 hours in each control room. In one control room -- I'm doing this off the top of my head -- there was something like two deployments related from 200 hours of observation, whereas in another there were over 20. And this was because of the different ways that they were related into the wider law enforcement situation, the radio links and the telephone links that they had and the relationships, the informal human relationships between those watching the screens and those responding to them. So it seems to be very important that we understand that this is more than just a technology. And it's incredibly variable.

That being said, let me now talk a little bit about the developments of CCTV in Britain. To sort of summarize, CCTV really enters the landscape in the 1960s mainly in the retail field. There are limited law enforcement applications. The first law enforcement application was monitoring a red traffic light, as we could see.

We saw a gradual diffusion in traffic in terms of monitoring some of the central London streets and also on the railway networks. And that gradual diffusion went on through the '70s. We saw more cameras deployed in mainly retail to prevent shoplifting and protect staff safety.

But basically, although the technology was there, it was only used in a very limited capacity. There was no mass expansion. And there was no main desire to develop open-street, town centre, high street systems. The first one of those occurs in Britain, as far as we can tell, in 1985 in Bournemouth. I think it's interesting to note that that also was a terrorist-related deployment.

I hadn't first understood this, but the cameras were deployed along the seafront in Bournemouth, which struck me as a bit odd when I found out about it in the '90s. Actually it was because the Conservative Party conference the year before at Brighton had been blown up by the IRA, nearly killing Mrs. Thatcher, killing five people, I think. So the next year they wanted added security and CCTV was found this way. Although it wasn't advertised in that way. It was advertised as generally for the town and a problem looking at normal crime in the town. But that seemed to be an exceptional case.

The trigger occurs in 1993 with the killing, the tragic killing of Jamie Bulger, a little two-year-old toddler by two ten-year-old boys. That image was caught by CCTV, a terribly grainy image that you could hardly make out. But it was replayed night after night on the national news. And there was a moral panic and revulsion around the killing of this boy. And CCTV in some way seemed to, well, at least encapsulate it. It certainly didn't save the little boy, but it meant we had some idea that at least we might be able to find the killers because of it. And, indeed, they were caught, partly as a result of the CCTV. But that event spotlighted CCTV in a public way.

Now it is not the only trigger. I think you'd have to look at a whole range of other social, and political, and economic factors which in a sense laid the seed beds for saying CCTV has a role here. But certainly at that time with crime going up, the fear about crime increasing CCTV seemed to offer something for politicians.

And the Home Secretary announced a very limited scheme. Two million pounds was put aside to sponsor CCTV schemes at the local level. You had to competitively bid for them. The scheme was absolutely overwhelmed by applications. The initial trunch of money was increased to five million, and that didn't satisfy the demand, 106 schemes to put CCTV in high streets was funded. The public money is absolutely crucial to the development of CCTV in Britain. I mean it explains a lot when in Britain you have much more CCTV than, say, in the rest of Europe because of the central government money that was put in.

And that money over the course of the decade just really in terms of open-street systems was about 250 million pounds, 85 million from the Conservative administration until 1996 and then another 167 million from the Labour administration.

So we've seen a huge investment. And that doesn't include the CCTV that's being deployed with public money in schools, on transport systems, in hospitals, and of course all the private cameras on garage forecourts, in retail.

It's probably -- it may be difficult for some people to understand quite the pervasiveness of cameras in Britain. There isn't a single space now that I can think of where a camera has not been deployed. And you might say: Well, they don't put cameras in toilets in Britain. But actually they do. If you go to railway stations in Britain there are quite often toilets in the wash areas of the toilets. They're not putting into the cubicles, but there are cameras watching you generally.

But actually in London police stations there are cells with integral sanitation facilities, a toilet, and there are cameras watching those cells. And there is no privacy screening. So there are cameras in a sense almost everywhere. You get on a bus, in a taxi, in a restaurant, in a pub, wherever. So there is a real pervasiveness. Nobody knows how many cameras there are.

I every now and again make estimates and guesstimates. And my last estimate a few years ago was there might be as many as 4.2 million cameras in Britain, one for every 14 of the population. I've spoken at various conferences to that estimate where industry people have been there and no one's actually said: You're wildly wrong.

In terms of what that means for an individual, I've also guesstimated that that might mean being filmed on 300 cameras a day, 30 different systems or so, although that estimates are made in 1999. And we've had a lot placed since then.

Okay. So we've had all these cameras. What do the public think about this? Has there been a great debate about privacy? No. I know of one single demonstration against cameras -- sorry -- against public town centre cameras. Speed cameras were a different matter. We will perhaps mention those later. But the two centre, there was a demonstration in the 1990s against the cameras in Brighton.

But other than that it appears that the cameras and the deployment of cameras enjoy a fairly widespread public support. Initially we were told from various sources that this was ranging in the 90 percent or 95 percent. Well, as always these claims tend to be a little excessive.

I think if you look at the good statistical material you see between 60 to 90 percent, depending on what question you ask, basically support the idea of cameras. I think if you ask, and I did in a survey, which I don't think I quoted here because it's not finally out yet, ask 200 Londoners whether they would welcome CCTV in their street. Somewhere over 60, 70 percent said they did. Whereas, if you ask the same of Berliners, you would get a very different response. In the main, though, then we have widespread public support. But this is actually stratified by age and gender. Men, particularly younger men, are less supportive of CCTV in public space than older men and women generally. So it's not quite even.

One of the interesting issues about public opinion is looking at the problem of attitudes and behavior, if you ask people: Would you -- if there were CCTV would people feel safer?

Generally what people will say: Yes, 70 percent will give support to that.

If you ask them whether they would feel safer, we find that only 30, 35 percent would concur with that sort of statement.

If we ask people before a CCTV system is put in place: Would you use the town centre more, you'll get 70 or 80 percent saying: Yes.

If you ask them after it's been put in place, you find a rather different story that, in fact, very few have changed their behavior because of the cameras. So public opinion is an interesting area. And I say broadly there hasn't been a major outcry about civil liberties, about privacy, or rejection. The public are broadly supportive of it, although one does have a view that their understanding and knowledge of the technology is actually rather limited. So it's unclear on what the basis of their judgments necessarily have been made.

Okay. So in the UK we spent all this money on cameras. So do they work? Well, what were they introduced for? We were told, of course, in the way it was presented politically and locally that what CCTV did was reduce crime, increase detections, and reduce the fear of crime.

And certainly in the early days in the 1990s there were in the media very strong claims of how effective CCTV had been. I can remember from one local study, which got a lot of support in the industry, a 95-percent reduction in crime. God, wouldn't that be amazing, you know, cut crime like that. And success stories abounded.

One of the things you know, if you've looked at CCTV or the implementation of it a number of years, at the local level you see this narrative. You see: We want to put it here because it's been a success elsewhere. And at the local level in publicity releases and press releases you see that. Then you are told in fact it's already a success here before we've even switched on the system because in testing we've already caught some burglars, and thugs, and so forth.

And then after the system's been introduced some two or three weeks or even a few months we're told how wonderfully successful it has been and success stories are showed, because the criteria of how we judge success has not been laid down. Merely if someone has been arrested and you can report that, that appears to be the evidence of success. There's no scientific basis for the judgment.

What happens when we look at the scientific basis for the judgment? Actually we start to see that the early claims made generally by self-interested practitioners are quite far from the mark.

The other crucial thing here that you have to understand is that there was no major evaluation funded by the British Home Office. Although they spent in the first traunch or caused to be spent 85 million pounds of public money from 1994 to 1998, they did not invest in any evaluation. Only the Labour Government after that had an evaluation, which was to run concurrently with spending 167 million pounds.

So what we found was actually, if you looked at the reasonable results, mixed findings. It worked sometimes in some places but not so well in others. There was some evidence of displacements, of crime being shifted elsewhere. In others there were evidence of diffusion of benefits, with the surrounding areas actually benefiting from the cameras and there being a reduction, too. But overall if you were a gambling man, you probably wouldn't have put money from that evidence on whether it'd work or not in a particular case.

If you look at the very interesting findings from the Scottish Office funded study of that time, which looked at two systems, Airdrie and Glasgow -- Airdrie being a small town outside Glasgow; Glasgow being a major international sort of city -- they found in a sense it worked at reducing crime in Airdrie, reduction of 21 percent and an increase in detections. Whereas, in Glasgow the same team, same methodology found crime rose to 109 percent its previous level, a nine-percent increase and detections fell.

So a complex story. If you look in -- in 1998 the Home Office eventually sponsored a proper evaluation or at least a properly-funded evaluation, about a million pounds. A large team working over four years to look at a range of systems, 14 case studies. Major public opinion surveys, crime surveys, and so forth. It's the best evidence we have.

What did they conclude? In terms of fear of crime, no impact. In terms of increased use of the streets, no impact. In terms of reduction in crime, basically no impact. You can read in the paper. It's a touch more subtle than that, but not much.

The best available evidence, not supported by another Home Office review, conducted by Farrington, which suggested that if you did a metro analysis of the most reliable studies on CCTV from a methodological point of view you found a four-percent reduction in public space CCTV, but that that was almost entirely confined to car parks. It didn't have an effect in city centre streets and it didn't have an effect in transport systems.

So the evidence is not very strong of CCTV as being good in the general level of producing reduced crime, fear of crime, or detections.

I think there's one other element we should just stress here is that, of course, that's just to focus on one element of CCTV, and that is as a crime reduction mechanism, because CCTV is far more than that, because it enables people to watch over other people and intervene in a whole range of situations that aren't necessarily crime-related.

One of the findings that came out of my studies and it's been replicated from a number of studies is that if you look at who CCTV operators look at when they have a joystick and the ability to zoom in and track people across a city centre on a range of cameras, is that they tend to target the usual suspects: Young, the young particularly; often the young from ethnic minorities; and often male, those dressed in baseball caps and trainers, and so forth, in a particular tie that signals some sort of association in the mind of the operator of criminality become the targets of surveillance. Not because of their overt behavior, merely because these people belong to a particular category, a category of someone the operator thinks is more likely to be involved in crime. And this then gives them the license in a sense to follow and track that person through public space.

And if we look at more recent studies that have looked at the operation of CCTV within the mall, shopping malls, we also find a strong exclusionary impulse, the same sort of people are looked at, but particularly those who are scruffy, who are seen as not very capable consumers, particularly groups of youths, are focused, not because they're doing anything wrong, but because they're destructing the image of a particular space. And then they are deployed against and ejected. So there are real consequences about the use of public and semi-public space.

Okay. I've talked mainly about the lack of its effectiveness and some of the drawbacks in terms of monitoring.

What then are the benefits of CCTV? I think one can't escape the fact that the symbolic benefit is huge. As a political symbol about doing something about crime CCTV was very powerful. It's also very public. They're putting up a camera; everyone can see it. Building a prison tends to be out in the country and no one notices it. It's running juvenile correctional facilities or youth offender diversion schemes don't. This was a very public thing. It also enjoyed public support. So it politically gave politicians at a time when crime was rising and they were having a difficult time a way of saying: Yes, we're doing something about crime. Here it is. It's in your high street today, as it were.

Also it provides a huge post-investigative resource. When things go badly wrong, when somebody is murdered, when a terrorist bomb goes off, those tapes, and there are now an awful lot of them, can be used. Those tapes can provide an evidential base, an investigative base, which is very strong. Although it also has a huge resource implication, too.

If you seize all the tapes from 400 video recorders across a district you then have to review them. In one case, we're talking about a team of detectives, over 50 of them, 13 days to go through all those tapes. So it's not a magic bullet having all that visual information, because somehow you got to use it. And when you've got systems that don't all talk to each other and you got different tapes, it doesn't necessarily work.

Thirdly, CCTV gives a whole new set of information to people who are watching, about low-level nuisance and behaviors that they may find interesting, such as local authorities or shopping mall owners.

For the police it provides a very useful operational tool for determining whether an incident that's come in from the telephone of two youth fighting, is really just two youths fighting, or actually a small riot's about to start. It gives them a way of actually rationally examining a scene and determining how to deploy to it.

And, finally, of course, where it exists, it provides very strong evidence. If you've caught someone red-handed on tape putting a brick through that car window, it's rather strong, particularly if you've got their face. And you tend to get a confession in those things so you don't have a lengthy trial. So it has those benefits. (Comments off the record re time left to speak.)

MR. NORRIS: Okay. Five more minutes.

Let me then talk about some of the developments that are occurring. I've talked almost solely about cameras. I think one of the really important things for the future is to think about the new capacities for CCTV. And that largely comes from the digitization of images and the coupling of computers with cameras.

What we're seeing in Britain is a deployment of cameras that I don't think many envisaged in the 1990s or even maybe five years ago, is the increasing use of cameras coupled to automatic license plate readers. So by using an automatic license plate reader, you can link a visual image to a record held on a computer. And you can start to use that for law enforcement purposes.

Now this was used originally, again, in a terrorist-related context in the City of London after the Bishopsgate bomb in the mid-90s to just monitor every car that came into the City of London, check its number plate against a list of wanted and suspect vehicles and then to determine whether to stop that vehicle. And that was in the context of a specific terrorist threat.

What we are seeing today is a new strategy, a strategy delivered by the association of the police, sort of chief police officers and the Home Office to deploy that nationally so that every car in Britain will have its -- well, not every car -- so that there will be a network of license plate readers around the country, some of those already existing in high street CCTV systems.

Every car that's captured by those cameras will have its information extracted and placed onto a database. That database will then be able to link it to the Register of Vehicle Licenses and then to the Police National Computer and all those other databases.

They are planning and what they have said they've done to be able to read 30 million entries a day into that database now, raising to 50 million in 2008. So what this means operationally is that you now have police officers, ANPR intercept teams, who are sitting with a computer waiting for a flag to come up to say a known or wanted vehicle has passed. Now that known or wanted vehicle may have intelligence related to it, it may be stolen, or whatever. And that then allows those officers to be deployed to that person. So the camera, by linking to the database, is providing the warrant to, seeing an offense, to intervene with that person.

In the trials of this, which were run in 2004, it lead to 10,000 arrests. The details are in the paper. But what's interesting is that 75 percent of those were not to do with traffic or driving offenses. They were to do with other matters which, I think, shows the power of the database.

Okay. Finally, because I only have about two minutes left, in the paper I review the legislation that is now in place, one of the things you have to understand is when CCTV emerged in Britain there was no privacy law that was applicable to CCTV. In a sense it occurred in a regulatory vacuum. It's only after 1998 when a number of laws had been introduced to bring it -- the Human Rights Act being one, which in a sense establishes more recently that there may be something called privacy in public and the Data Protection Act, particularly, are most important, because the Data Protection Act gives codes. It gives the codes of conduct that systems are supposed to use so they are compliant with the Data Protection Act.

I don't have time to go into the details of that. And I'll think I'll probably just stop there and let the Committee ask questions and can reach the end.

MR. BEALES: Thank you very much. It was a very interesting presentation. And I'm sure we'll have lots of questions, and we'll start with David Hoffman.

MR. DAVID HOFFMAN: Thank you very much for coming and speaking with us today. I read your paper a couple of days ago, and I found it to be absolutely excellent. To everyone in the audience I would highly recommend giving it a read.

I thought your talk today was very interesting, and it painted a great picture for us of the history and the development of CCTV and where we're at today. I'm wondering if you could talk for a couple of minutes on your thoughts of where we're headed in maybe the next five years, especially on technological advancement. You talk in your paper a little bit about where facial recognition is today. And I'd like to hear your thoughts on where you think that might be in four or five years and also where we're headed on integration, since storage costs come down so much that whether you can integrate data together from different systems.

MR. NORRIS: Okay. Thank you.

One of the key problems that's occurred in Britain is we've all these little systems sponsored by local and central government. And, of course, the running costs of that's huge if you're going to monitor them.

What's happening now is you're seeing the emergence of much bigger control rooms, control rooms that integrate a whole range of functions, functions of both the public from -- public and private sector. So you're seeing, in a sense, the professionalization of the control room.

You're also seeing much -- a move towards digitized systems, not fully in some cases, but that is coming on. You're starting to see, therefore, the integration with those with some of these new technologies. For instance, facial recognition and behavior recognition. In terms of facial recognition, I've been following facial recognition for a decade now, a lot has changed in a decade. But in terms of public street CCTV, in terms of being able to recognize a face in a crowd, it is really, really difficult. And in terms of security terms where it might be critical it is actually -- it is not a technology that is viable.

In open-street situations where you have limited access control situations, where you have a camera from that space, yes, it works. I really am not sure -- if you say five years, my view is in five years I don't think we will be there to be able to recognize a face in a crowd.

It will be interesting to look at the next evaluations, the officials that are American government-sponsored evaluations of facial recognition. And there's one being conducted as we speak, I think, because they do provide some definitive tests.

In terms of behavior recognition, it's very difficult to say. There are limited algorithms for determining what is suspicious behavior. I mean they don't seem to have entered into the sector. It's very easy to determine if a vehicle is going the wrong way. And that's happening a lot in vehicle recognition. So with a camera you can see a vehicle is going the wrong way. That means that you can then determine that that might be a threat, set an alarm off, deploy people. But in terms of more general surveillance I'm really not sure about that yet.

MR. BEALES: Tara.

MS. LEMMEY: I'm curious about whether your studies or studies that you're aware of have dealt with the chilling effect on people's behavior in public spaces. Are they less likely to attend demonstrations? Are they less likely to participate in normal behavior because of the camera placement there?

MR. NORRIS: My studies haven't addressed that issue. One of them tried to but unfortunately the place I was looking didn't install the cameras in time and the funding ran out and we did something else.

It's certainly an area that is posited, that if you know that your image is going to be recorded that you will -- that there will be a chill and people won't use public space because they think that they're under observation and suspicion.

I don't know that there's strong empirical evidence to support that, but I think everything if we -- well, there is -- I don't know any empirical evidence that actually supports that claim.

MR. BEALES: Sam Wright.

MR. WRIGHT: Thank you for your presentation.

Privacy has a lot to do, a significant element of it, with expectations of the individual as to what's an invasion of privacy and what is not. I'm just curious. In Britain how much is being done either by the government or other public agencies to disclose to people, to put them on notice, to make them aware of the fact that they are in a public space that is under surveillance and just how that is done, by signage, or by public notice, or other devices.

And then, secondly, if you have any information concerning the number of cameras or systems where there is active monitoring of what is going on in a real time basis as opposed to those which are just being recorded and stored for potential examination later.

MR. NORRIS: The issue of signage. Under the 1998 Data Protection Act part of the issue was if you're collecting personal data, and CCTV images were seen as that, there's generally a view of consent needed to process that data. Given that you can't have that in terms of CCTV, we cannot suddenly sign a form, the view put down from the Data Protection perspective was, therefore, we had to at least be notified that we were under surveillance.

And so all CCTV systems under that Act, whether in public or private space, if they were monitoring us, had to have signs, they had to register with a Data Protection Office and they had to adhere to the codes of conduct, all those elements that were in a sense legally forcible in terms of data protection. The problem was that in our study, where we actually looked at systems in one London borough, only 22 percent were compliant with the signage regulations. Now that may have gone up now.

A second issue, which I'm afraid isn't in this paper, because it's only just -- it was an oversight -- is that there's been a recent ruling which actually said that if you're merely watching someone and not tracking them, you're not processing personal data, therefore, you don't come under the Act and, therefore, you don't need signs or to register with the Data Protection Office. So that's -- the signage issue is important.

In terms of how many of them track, we don't know how many cameras there are. We don't know how many systems there are. There are somewhere in the region of probably five or six hundred public town centre systems which are at least monitored and use tracking through part of the day. And I would expect that there are at least 150 that are permanently 24- hour monitored major city systems. But, of course, then you have the underground systems, and so forth. But we don't know the answer quantitatively.

MR. BEALES: Joe Alhadeff.

MR. ALHADEFF: Thank you.

I guess mine is a little bit of a following question based on the last part when you were looking at some of the benefits where there -- and it seems to be after the terrorist incident in London and seemingly the quick identification of some of the suspects that there is now a large focus on the after-the-fact benefit as opposed to any of the potential-for-prevention benefit, which seems to, by your evidence, not have been borne out as a prevention benefit.

I was just wondering, in your analysis of the cameras, was there a concept that a targeted use as opposed to this 44 million or however many million cameras it was, blanket use of the cameras, but at a targeted use of the cameras for after-the-fact issues may actually have success with some sufficient benefit to warrant the potential intrusion that they cause?

And then the second part of the question was: We heard an example of misuse in terms of those people in a mall tracking the behavior of people just based on ethnicity, or their appearance, or lack of credible consumerism. But I was just wondering if there were other examples of misuse of information or if things like the Data Protection Act have been successful in making sure that uses of the information have been at least compliant or neutral and not to wrongful ends.

MR. NORRIS: I forgot the first bit of your question.

MR. ALHADEFF: The first bit was the concept of a more targeted use of cameras for after the fact and whether there could be a benefit there.

MR. NORRIS: I don't think you -- I think it was there implicitly, but I don't think it was a strong public view that it would be found useful. I think it demonstrated itself to have some use. But, as I say, the problem with the after-the-event thing is that where it presents itself to you by good fortune, as it were, someone does put a brick through the jewelry shop window in front of the camera and their face is clearly recognized, great, it's a wonderful thing. But actually often it's much more complicated than that, because although you've got the image of them putting the brick through you can't see their face properly because they're turned the wrong way, or they're wearing a hood, or whatever.

So that after-the-fact benefit is often very expensive because you're actually trying to investigate, but often very worthwhile. So it's, you know, it's about critical instance. And some of those critical instances are really important. But I don't think that was explicitly seen as a justification for their, their use.

And so your second question?

MR. ALHADEFF: The second question had to do were there examples of misuse beyond the person wrongfully tracking, or do you think some of the laws have actually been effective in controlling use appropriately?

MR. NORRIS: Well, certainly in the early days of CCTV there was -- there were a range of disclosures from systems of -- from public and private systems of people doing things in the streets that they perhaps shouldn't be doing, sometimes with other people consensually but not many clothes on, and so forth. It appears to me they seem to have dried up. They do come out every now and again. But in the main they've dried up. I seem to remember in the early days, in the '90s, there was a picture of Princess Diana, for instance, in a private gym doing exercises which had very close-up shots. That seems to have slowed down a bit. And I think the Data Protection Act has done that, and I think public systems in the main have got their act together about these things. They made a disciplinary defense sackable to this unauthorized disclosure, and so forth. So the Act has worked in some ways.

And I think the important case here is back in terms of human rights where a London counsel gave footage of a man who had attempted to commit suicide to a film company. They did not manage to ensure that his face was properly blotted out before they gave this footage. It appears this was a mistake. The result was that his image was broadcast in the trailers for the documentary on national TV at prime time and in the documentary without -- not in all occasions his image being blocked out.

So this, it seems to me, one of the dangers. They argued in a sense that this is legitimate; they were showing the benefits of the system. He argued that his privacy had been grossly invaded. In Britain at the time no English court could find that an invasion of privacy had taken place in law because we had no privacy legislation. That changed with the Human Rights Act.

When it went to the European court, the European court did find a breach of privacy in quite a limited way, and some people have argued the judgment isn't as strong as one may think. But it does at least establish that they shouldn't have broadcast it to the nation, as it were. But in Britain it's still very unclear about if something is in public whether you can take pictures of them and distribute them.

MR. BEALES: Well, we may not have a Data Protection Act here, but one thing is clear, that was invasion of privacy under U.S. law.

Richard Purcell.

MR. PURCELL: Mr. Norris, we've heard a lot about the state of play for CCTV in the United Kingdom. What I'm curious about and perhaps other Committee members would be perhaps curious about, as well, what do you recommend? What's your judgment of -- after a decade of following this issue and seeing it evolve, where do you see it going and what kind of recommendations would you make for other cultures, not necessarily -- I mean the UK has got a saturated environment, but there are those who don't and are considering this. What recommendations would you make?

MR. NORRIS: I think, firstly, I would say you need to do this on the basis of good evidence. If you're going to put cameras in and spend public money doing so, there ought to be a good rational basis for it. It seems to me the cameras can, in certain situations, help alleviate particular problems, particularly when utilized in relationship with human monitoring, increased security, changes in design. And so we have seen in car parks this can work very well.

If one thinks that CCTV will be a magic bullet to the problem of crime or terrorism, in my view, it will not be. So one needs to think very carefully and critically and scrutinize whether these systems are actually justified in the terms that they are being put forward.

The second point I would say is from my personal perspective and what's at stake here is that you have to understand that it seems to me that having CCTV in place changes the power relationship between watched and watcher. Normally when we're on the street, we can see who's watching us. We can change our behavior because they are watching us. We can leave that space because they are watching us. We get a sense of what Guffman calls, we can defend the boundaries of ourself, the territories of ourself.

And we know actually there are strong social expectations of privacy, because in these things the spy and voyeur get universal condemnation because they hide their intent and they hide the fact that they are watching. And they offend us because they don't allow us to know that we are being watched so we can alter our behavior because of that, or we can interact with them at least to challenge their gaze.

When you put a camera up there, it changes it. It changes it fundamentally, because we no longer can see who is watching us. We can no longer challenge them directly to stop looking, and we know how many fights are started because, "Are you looking at me, mate?" Yeah. We know these rules intuitively.

So that being said, we have to say there's asymmetry of power going on here, which disrupts our normal expectations of the street. In the paper I say it seems to me there are three key things. The things are: I think at a base level people should be made aware of the cameras. And that seems to be regardless of whether you can track and zoom and so forth. So in England we've just seemingly diluted that ability, because if you can't track and zoom and you're merely recording it appears you don't have to put signs up. It's a bit unclear, I must admit, but that appears to be the state. But it seems to me we should allow people the right to know they're under surveillance.

It seems to me that we should have rules to say the images should not be divulged to anyone except in the case, in the exceptional case of the need to prevent or detect crime. And I don't mean to deter crime. I mean to actually prevent a particular crime and to detect a particular crime. So you can't just use it as publicity material. It's got to have a specific worth.

I think thirdly -- and I think this is important -- I think the Data Protection Act was never meant to regulate cameras in Britain or in Europe in a way. But it's not legislation, data protection legislation in a sense it has fallen to. I think in that sense as a model it is trying to do it quite well. I think the codes of conduct issued by the Information Commissioner are sensible. But actually they're largely concerned with allowing CCTV to operate in a lawful manner. They are not concerned with restricting it in the first place. If you can say: I'm going to put up a camera to prevent crime, it's legal. That's in a sense as long as you use it in that way. If you use it to spy on your neighbor it would be illegal. But it doesn't try and restrict it.

So we have the Data Protection Act. I think it does a reasonable job but it could be better, but it's very difficult to enforce it. So enforcement is very weak. And I think this would be true in many regimes. We pass privacy laws or data protection laws, but we don't fund the enforcement mechanism to deal with it. I think that if you're going to use that mechanism then, for instance, data protection officers should have the power of inspection of CCTV systems. They don't in Britain. There has to be a complainant first.

I think that is important. And I think they need to be funded at such a level that they can actually make -- they can ensure compliance. If the public, if there is this power in balance, I think the public have the right to know that these systems are run fairly and in accordance with the law. And to do that we, therefore, need some form of mechanism to guarantee that to them rather than systems merely saying: We comply, because they'll always say they comply, but the question is: How do we know they do?

My final point in terms of -- and I did think long and hard about this, because we don't know what the future will hold -- is what should we do? Well, I think we have to start thinking about -- well, I think one possibility is to allow citizens the right to know what information is held about them.

Now that sounds really innocent, doesn't it? It sounds like a classic, but it's in data protection. But I want to go a bit further than that. When I say "allow [them] the right," I want to change that right more to a duty on the possible authorities to actually present an information statement about what information is held by them and how it has been used.

Now this is particularly in the case, it seems to me, where you have nonconsensual use of information, such as in CCTV or in my license plate reader. We didn't consent to this information being used. So it's about the asymmetry of power again; it gets it.

Now that, of course, raises a question for many of the issues I've been talking about, because the information we're talking about is law enforcement information. It might be anti-terrorist information. So am I really proposing that we should provide such people with information or let them know what information is held about them? And in a way, yes, I am saying that those people in a sense have a prima facie right to it, which we then might want to interfere with.

The question then becomes this: How do we decide what information shouldn't be given to people? After all, it's their personal data. And there may be, indeed, very good reasons for not giving certain people information about what's held.

But given that in the British case it appears that those records are now going to be held on every motorist, our location and time, in points of time, our associations as the software is used to track which cars were near ours on Christmas Day and Boxing Day, or whatever. You know, these now seem to be real threats.

So that would be my response. I think we need to think rather more actively about the asymmetry of power and how we can try and redress it, particularly when consent is implied.

MR. BEALES: If I could just interject. It's sort of a -- sort of a follow-up question, I guess.

You're talking about CCTV as a system. And in some ways it clearly sounds like that's exactly what it is in Britain. In a lot of the U.S. applications there are some very restricted applications. I'm thinking, for example, taking a picture of whoever is engaged in a transaction at an ATM. You know, there's sort of very -- okay, if it's a bad guy, we want to be able to figure out who it was, very focused that way, or the security camera in a bank lobby that, you know, has the same sort of pretty narrow focus. It doesn't go anywhere else unless there's something after the fact.

Would you distinguish between that kind of system and the street camera, or do you think they ought to all be treated pretty much the same?

MR. NORRIS: Well, I think you have the right to know that that camera at the ATM is taking your picture. I think, you know, I think that's reasonable. It should be stated it is. After that, I'm not sure. I mean, you might want gradations of things. That's why I say we don't want to treat it at as one thing. We need to think carefully about it.

On the other hand, if we do agree that what they have is personal information then, of course, they do because they can link that to your bank account, you know, if it's an ATM situation. Then we might want to say we at least want to be assured that the processes that you use are safe and, therefore, you should come under whatever law it is and there should be some power of audit to make sure that that is being used reasonably and not unreasonably. But there are horses for courses. And I mean, that's the difficult thing.

MR. BEALES: Our last question. Ramon.

MR. BARQUIN: Now as you started to talk about the future and the digitalization of the recording, specifically with your example on the automatic license plate reader, the question of data integrity then becomes extremely important. And I wanted to see if you had some comments both on what might have come up on these trials and what you're thinking about doing in the future.

MR. NORRIS: It's a -- well, my thinking of --

MR. BARQUIN: Of what the thinking is in the UK vis-a-vis this issue for the future?

MR. NORRIS: The issue of data integrity?

Well, it's interesting you asked that. This has been a major problem. It's been a -- the integration of ANPR, automatic license plates, into the system is only one element of in a sense a much more intensive focus of using proactive methods to investigate crime in Britain and a huge investment in a range of database technologies and expansion of the police national computer, particularly in an upgrade of it. So this is part of a much wider thing.

One of the things that has come out of that is the problem that the records are so poor. There is an inspection report by Her Majesty's Inspectorate of Constabulary called, "Under the Microscope," which I can let you have the reference for after, which shows just how awful, in some cases, this is. And, indeed, it's a question that has been raised by the Data Protection Office in Britain of the police databases.

Clearly, if you're going to use these databases, it is absolutely essential, particularly if they start becoming intelligence files, I mean it's this cross-linkage between different things, that this data is accurate.

All I'm saying is this is of serious concern to the government and various agencies. They are investing a fair amount of money, time and resources, and administrative clout to try and do something about it. And it is recognized as a data protection issue. I hope that goes some way to answer it.

MR. BEALES: Mr. Norris, I want to thank you very much for joining us today. This has been fascinating, and we really appreciate your being here and answering all our questions. According to our schedule, it's now time to end our break. I think, rather than do that, we should take an abbreviated break. And if we could come back at 11:10, we will resume then. And I think probably squeeze either lunch or subcommittee reports, depending on which squeezes best. And so 11:10.

By the end of the break, if you want to speak at the public hearing part at the very end, you must have signed up. And we will figure out how many people we have and how we're going to deal with it. But that's the absolute cutoff for signing up for public comment.

Thank you. (Morning Break)

MR. BEALES: Our next speaker is Mr. Steve Yonkers. He is the Privacy Officer of the US-VISIT Program of the Department of Homeland Security. And before joining US-VISIT, he was a Program Manager with the Office of Internal Audit for the INS and with the Office of Community-Oriented Policing Services and with the Bureau of Justice Assistance.

Mr. Yonkers.

US-VISIT – THE ADVANTAGES OF USING RFID IN THE IMMIGRATION AND BORDER MANAGEMENT ENTERPRISE: MR. STEVE YONKERS, US-VISIT

MR. YONKERS: Thank you very much, Chairman Beales and members of the Committee. Thank you very much for having me here today.

I'm looking forward to talking a little bit about the US-VISIT Increment 2C, which is the proof of concept that we've been using, using RFID-embedded I-94 Arrival-Departure forms currently at five land border ports of entry.

I'm also hoping to talk a bit about some of the conclusions that were drawn in the Draft RFID Report and, maybe more importantly, talk about how US- VISIT and DHS are working very hard to protect people's privacy, make sure we really share accountability, provide responsibility, Department-wide, and really make people understand that protecting information, protecting personal privacy is really a fundamental part of how we do business at US- VISIT. It's an integrated part of the system development lifecycle and it's part of everything we do.

In fact, in terms of US-VISIT goals, we have four goals for US-VISIT. The first is, as you could expect, is enhancing the security of both our citizens and our visitors.

Second is also the facilitating legitimate travel and trade. We recognize that we can't shut down the borders, that while we're enhancing security we have out make sure that travel and trade continues, that people can come in, visit family, come here for business, come here to go to school as well as commerce. We need to make sure that we don't shut down commerce or create economic chokepoints.

And a third goal is ensuring the integrity of our immigration system. That's a very important goal. One of the fundamental goals of why US-VISIT started a biometric entry-exit system was so that we can better know that when people arrive here and then when they leave that they're doing so in compliance with immigration requirements, that we could do a better job of understanding who is coming in and making sure that people aren't overstaying beyond the terms of their admission.

And then, fourth, our fourth goal is protecting the privacy of our visitors. And that's really done in concert with the other three goals. And it's just a fundamental part of each of this. We understand that if we do just one or two of these goals, if we don't do all four goals in concert, then we're not going to succeed, we're not going to build the trust that we need to be successful, and we're not going to be able to keep moving forward. Now over the past two and a half years, US- VISIT has successfully implemented biometric space into processing at all air, sea, and land ports of entry. We've also moved US-VISIT processing out to the Department of State Consular Offices abroad as part of the Department of State BioVisa Program. And that is what enabled us to enroll people into US-VISIT while they're still in their foreign countries, while they're still applying for a visa and, therefore, be able to collect their fingerscans, digital photograph, and other information; compare that information against watch lists, know that they're good people, that they're going to likely comply with the terms of admission.

And then when they arrive at a POE, they're already pre-enrolled and we're really just re-verifying, making sure that this is the actual travel document that was issued to them, that someone else isn't using it, or they haven't tampered with the document in some way, and this is the same person that the document had been issued to. And those are things that we're currently able to do with the US-VISIT process.

Now during the past two and half years we have published numerous privacy impact assessments. In fact, that's one of the key parts of our privacy program, is the notice aspect, which is before you roll something out, getting that advance notice out to the public saying: Here's what we're planning out do. Here's the type of personal, identifiable information we're planning to collect. Here's how we're going to be using that information. Here's how we're going to share that information. So we can let people know ahead of time what they're going to be asked to share with us and how we're going to be good stewards of that information.

During the time that we published our PIAs -- the good news is most people reflected upon us and including many privacy advocates have noticed this was an excellent model for transparency, particularly for a Department of Homeland Security initiative, to be able to show that we're going to be out and open as much as we can about what we're collecting and how we're using that information.

And what's more, we're going to be forthcoming in identifying the privacy risks that we see at any given time. And we're going to make sure mitigating those privacy risks to the lowest level possible. I think we all know that we can never totally eliminated privacy or security risk. It's just not reasonable; it's just not possible. But we can and should minimize privacy and security risks to the lowest level possible in everything that we do.

Now in terms of implementing 2C, the proof of concept where we're actually embedded RFID tags into I-94 forms. And it's first to note that this is a proof of concept. It's not a pilot test; it's not a full implementation. This is really our very first opportunity to look at, given the challenges that we have at the land borders, to what degree, how well will RFID help us meet those challenges. And also can we use -- to what degree can we use RFID in a thoughtful manner that protects people's privacy, that we're not putting people's personal identifiable information at risk and that we're not inadvertently creating privacy risks that we hadn't thought about.

Now we talk about the land border. If you haven't been to a land border, it's probably difficult to understand what the problems are, so I'll try to give you some sense of that.

First of all, we have, approximately, I believe over 300 million people coming into the United States every year through land ports of entry. In fact, over 80 percent of all travelers entering the U.S. every year do come in through a land border.

Now as you now land borders provide the important flow of goods which is very vital to our economy. They also provide the means for people who live in those border economies to go back and forth for business, for pleasure. Many people in Mexico own homes in the United States, and vice versa. And so for the people who lived on the border their whole lives their expectation is to be able to freely cross any time that they choose to so long as they're meeting immigration requirements.

And one of the key things for us was to make sure that we're not disrupting that. We spend a lot of time doing a very extensive outreach program with these border communities talking to the people, to associations, to businesses, to landowners who said: We don't want you to disrupt this flow. Yes, we understand you need to implement additional security protections and we're willing to work with that, but we also want to make sure that we can continue the flow, that you're not going to shut down the borders, you're not going to make our lives much more difficult.

Now with the current land port of entries, most of these ports of entry have been there a long time. Most of them have not been updated. Many of them still use paper-based procedures and manual data entry, both for entry as well as exit.

When we rolled out what we call Increment 2C, which is when we first rolled out US-VISIT to land ports of entry one of the first things that we tried to do is start automating as many of those processes as we could, and those made fundamental improvements. But, where we rolled out to land ports of entry for Increment 2B, that didn't affect the majority of the population. There's still the majority of the people who are not being processed through US-VISIT and could not really receive the benefits of that.

So when we look at what are the next steps of the land border, our goal is not only to make sure that we're doing a biometric entry and exit recording of people at the border, but we want to make sure that we're actually transforming the entire inspections process. And that's maybe a part that most people don't understand, which is we're taking a more comprehensive look at how are inspections conducted at the land ports of entry in saying: How do we reengineer this entire process to the degree possible?

We know that we're limited in making infrastructure changes; we know that there's great environmental concerns about expanding the presence of the land ports or making people wait longer in line and creating more pollution at the ports.

We know that we don't own the land surrounding the ports of entry, and we can't just go out and buy more land. We're very limited in making additional acquisitions. We don't own the bridges. So we're very limited in what improvements we actually can make at a land port of entry.

Now in terms of the Increment 2C, proof of concept and, again, working with the land border communities, looking at how can we reengineer this process, how we can provide more critical information upfront for the CBP officer and at the same time facilitate trade and travel, one of the things we looked at first is, when we looked at what type of technology, we said what we want to be able to do, as you're cuing in line, as you're approaching that CBP officer inspecting booth is, instead of waiting until you're right in front of the CBP officer and then presenting your document, if you've got a carload of four or five people -- I mean, it's four or five people that are going to have to pass forward their passports, hand them over to the CBP officer who's going to swipe each one individually. Each one is going to require a processing time to retrieve the traveler's record, conduct any watch list checks with a spirographic and/or biometric and return all that information to the CBP officer.

If any of these people are wanted or now have become a known threat to the U.S., the CBP officer wouldn't know that until he or she had already begun interacting with the person in the car. Not exactly the best situation for the CBP officer to be in.

What we said is as you're cuing up we want to be able to preposition that information. We could not conduct any watch list checks ahead of time. So if there's a hit, we already know that we could put together some type of response. But, even more importantly, we want to be able to preposition the data and not really require anything additional for the travelers in the car to have to do. We did not want to have to have them roll down their windows in the middle of the summer and reach out the window and try to scan or run a travel document against some device that's put in the lanes.

We don't have a lot of ability to add things into the lanes. We did some time-and-motion studies and found it would be much more time-consuming for people to be sticking their arms out windows and trying to scan one document after another. That's why we looked at RFID. We looked at active RFID. We looked at passive RFID. We even looked at GPS. We even looked at the possibility of making it more like the airports and seaports, where when you come up to primary, you actually get a new collection of your finger scans and a brand new digital photograph taken. We looked at that possibility. But in the alternatives assessment that we conducted, we determined very quickly that while things like GPS and active RFID would be extremely helpful in meeting our mission needs, it would not be very good for meeting our privacy needs. And making sure that we're embedding privacy in the process was one of the guiding principles when that assessment was conducted.

And as we looked through each technology we kept saying no to different technologies really up until we got to passive RFID, which we said: This will allow us to preposition the information. We're not going to put any personally identifiable information on the RFID tag itself. It'll allow us to put that information ahead of time, preposition it. It really minimizes the privacy risk, especially as compared to the other type of technologies available to us. And at the same time it'll help us not only pull up the information from the database, but also provides that electronic entry to record entries and exits.

Now we know that entry is very different from exit. With entry, you're going to make the stop. You're going to stop in front of the CBP officer; you're going to go through the inspection process.

If you need an I-94 because you have a visa or if you need to stay beyond the requirements of the border crossing card, then you're going to go to secondary inspection, which is going to be a little more time consuming and you're going to have to go through that process.

Exit is very different. Right now people leave pretty much at speed, as we call it. In fact, we looked at anything that we put in place, we did not want to disrupt the flow of people being able to leave at speed, up to, say 40 miles an hour as they're leaving the checkpoint.

So when we looked at both entry and exit, we wanted to implement technology that could be the same technology used in both places, both for entry and for exit.

So all together, in terms of what the proof of concept is trying to accomplish, we're looking at providing more timely, more complete and accurate information to the CBP officer while minimizing any additional burden on the traveler, while minimizing any additional waiting time for people trying to get through.

In terms of protecting then travelers' privacy and PII obviously when we first looked at this, we said: We don't want to put PII on the card. We don't want to put it on the RFID tag. Let's keep the personally identifiable information in the secured DHS database where it belongs. Let's make sure that the RFID tag is really just providing that trigger. It's giving us an opportunity to pull up that information in a secured place. The personally identifiable information doesn't travel amongst the airwaves. Someone could not intercept this information as it's going to workstation. That was very important to us.

As we conducted our privacy impact assessment for 2C, which I would note was published on July 7th, 2005, we discussed how passive RFID was selected amongst all other available technologies. But one of the key things we wanted to make sure people understood is that we are not using RFID to track people. RFID is not being used by the Federal Government for surveillance. It is solely being used for pre-positioning that information at the port of entry.

Now in terms again, as the tag itself, I just want to remind everyone that there is no personal identifiable information on the RFID tag. What is on there, though, is a unique serial number. That serial number does not contain PII, nor is it any -- nor is it derived from any personal information.

Now the fact that the RFID tag number is unique does present some risks, and those risks were discussed in our PIA. And what we noted is that there is a low risk, based on the way the technology works today, based on the readers that are available and what we know about the technology and how it works, there is some low risk that if someone had the right rogue reader set up in the right locations that they could possibly skim that tag number.

But one of the things we realized when we looked at that risk in trying to identify is this a low risk, a medium risk, or a high risk, just how big of a risk, how plausible is it really for this risk to occur, one of the things we realized is that the RFID tag itself, when it's being read, emits a non-directional signal. What that means is if one of you had a reader right now, and if I had that RFID-embedded I-94 tag in my pocket so that you couldn't see it, even if you could read the number, you would have no way of knowing that I'm the holder of that tag. With all these people in the room there would be no way to associate me with that RFID tag with that number that I'm holding. And that's very important.

In fact, how would you get that tag number? Well, you'd probably have to triangulate it. You'd probably have to have a reader in front of me, behind me, and on the sides. And that's assuming there aren't a number of other people in the room that also have RFID tags on them also being read at the same time by these readers because, again, it's all non-directional.

The only way you could really ensure that you're associating the tag number with me, Steve Yonkers, is to have me walk through an alcove or a doorway that's been situated so that it's only reading everything within that alcove space. Is that likely? Are we seeing that happen? No. It's not very plausible. Is it possible? It could be, which is why it still remains as a low risk.

The other part about RFID signals is that they're easily disrupted by either bodies of water, meaning the human body, or metallic objects. And so one of the things that we looked at, and we tested this, is if I have the RFID tag and I have it in my shirt pocket, will you be able to read that number? The answer is it's extremely unlikely that you're going to be able to get a read of that number because it's so close to my human body, as a body of water, I'm going to disrupt that signal.

Now I've heard people say that's not what they heard from the other experts, but this is as a result of our tests.

Now having said all that, we recognized that the technology is always improving, that they're making better readers all the time; they're going to be more powerful. But they're also improving the tags themselves. We're using a UHF generation 1 tag for our proof of concept testing. Already now it's available, a generation 2 tags. This offers enhanced privacy and security protections against skimming, eavesdropping, and the other tests of vulnerabilities associated with RFID tags.

When we move beyond this proof of concept testing, we're definitely going to move to this next generation of technology. And even if we keep looking at the risk of the tag number being skimmed, and keep seeing that as a low risk, we're still going to employ additional mitigation strategies because, really, while we can't eliminate the risk, we want to continue minimizing it to lowest level possible.

What I'd love to be able to say is if you have that RFID tag in your possession, there is almost no way that anyone could ever get that signal. I always want to be able to say that as a privacy officer. I want people to feel rest assured that they can carry this RFID tag with them at all times and not feel like they have to leave it at home or that they're going to be subject to some type of surreptitious surveillance. We want to be able to say that we're constantly scanning the vulnerabilities and we're making sure proper and reasonable mitigation strategies are in place.

I think that ends most of the comments I wanted to add today. We appreciate the Committee's interest in the work. As I said, we don't necessarily agree with all of the conclusions that were reached. We think it's a little too soon to say that RFID should be disfavored. We believe, for the application of the Increment 2C proof of concept it's actually an excellent application of RFID for that limited purpose. And we will continue, through our privacy impact assessments, through systems of record notices, updates as necessary, that we're going to continue to be transparent about that. And we also encourage anyone who believes that they're seeing vulnerabilities that they think we're not seeing, we'd like to talk to those people. We're interested in hearing what they have to say.

We're constantly doing testing, but we're not going to be know-it-alls up here. We're going to be open. We're going to continue to conduct outreach, and we're going to continually be looking for feedback because in the end even if we are a hundred percent right on all the facts, the vulnerabilities, and the mitigation strategies, and this being the right technology for this type of application, perception is critical to the success of our program. And that means that we need to be able to make people trust us. And that means we have to be transparent, and we have to be out there and let people know: Here's what we're doing, here's how we're doing it, here are the steps we're taking to mitigate the risks, and then listening to people and getting their feedback.

And with that I'm happy to take any questions that you have.

MR. BEALES: Thank you, Mr. Yonkers. We have time for a couple of questions.

I guess we'll start with John Sabo.

MR. SABO: I think my colleague Lance was a bit ahead of me, but a quick question.

Steve, it sounds like what you're saying is with respect to the RFID tags' utility at the border, the primary utility is speed of exit because the entry requires an interaction with an immigration officer or inspector. Is that a fair...?

MR. YONKERS: I would say it's actually both. With the pre-positioning of data, with being able to bring that up ahead of time, the difference is having that information, having that computer processing already done and completed before you start the actual inspection encounter with the CBP officer. Every time we've looked at it, that saves times and that's going to make a qualitative difference even on entering.

MR. SABO: The other thing, given the talk from the speaker on CCTV, have you explored the future unintended consequences of the deployment of RFID? Generally we're now looking at RFID in passports. If, even an encrypted serial number on an RFID tag can be read ultimately, it could be used for surveillance, is that not correct, even if it's encrypted you may not have the actual encrypted number, but you will have probably a unique encrypted field of data being transmitted. So have you looked forward at this issue and can you talk a bit about that?

MR. YONKERS: We have -- we have been looking at that specific issue right. The question is: Even if you've encrypted the information at some point are you actually going send something in the clear which will allow that then to be eavesdropped and then use that to associate the tag with the individual. And our understanding of what's going to be available with the Gen 2 products if the ability to even be able to secure those transmissions to where it's almost like a PKD-type infrastructure where nothing is ever going to be in the clear. And so there's actually going to be a tag involved or, I should say, a key involved that would be used to unlock the information and, therefore, even if you're sitting in on the entire transmission you still would not be able -- you may be able to get it that one time, but then it's going to be constantly changing. And so the next time I used my RFID tag number, it's going to be different information being transmitted back and forth.

So is that a complete mitigation? That's something we're still evaluating. But it looks very promising.

MR. BEALES: Lance Hoffman.

MR. LANCE HOFFMAN: You mentioned that -- you got my interest especially when you talked about being able to scan or not being able to scan a tag on a shirt pocket, or something like that. And you properly said that we've heard different things from some other experts on what is scanable and what is not.

What is your policy of making the technical test, the technical reports public? I do understand that you said you have to be transparent, you want to be trusted. We all agree, but unfortunately this sort of reminds me of a lot like the voting technology concerns, which we've seen right here in this area where the Alameda County results, for example, came in very late today because the election yesterday couldn't use all these expensive machines they bought because they had believed one thing and then there was enough of an uproar that they had to go back to paper ballots.

I'd like not to have that same thing happen with DHS where a system is put into place only to be stood down. Can you comment on the transparency and the policy of making the purely technical reports public?

MR. YONKERS: Absolutely. I think you're right. An important part of transparency is making information available to the public and going through that process. Certain things are going through an internal clearance process and of course that may make things not as readily available as you would like, but at some point things become final products and those should be able to be released.

We recently made available, I believe it was the last couple of months, we put up on our website the actual 2C Operational Assessment Document, and that's available for everybody to read. And that will explain the different types of technology to look at and how we came to the conclusion to choose passive RFID for that implementation. There's probably other documents, I'm sure, that people would like to be made available.

And I think that's incumbent upon us to go back and say, okay, we've spent a lot of energy making our case to the Department, to OMB, to Congress to actually move forward with all these initiatives. But we need to make sure we're also making the case to the public. And that's probably going beyond just outreach activities and having good PIAs and SORNs being published, but also putting more information up on the website.

And that's one of the things I'm going to do when I get back, is go through and say what can we immediately release, what can we start getting up there right now. And even if we can't release an entire document, there's probably results from time- and-motion studies, all the statistics from the demonstrations that we've ran. They'll probably be very valuable in making people feel more assured that really did look into this, that we're just not seeing it because it sounds good. But we're seeing it because we tested it and because that's what we've determined to be true. So I totally agree with your request.

MR. LANCE HOFFMAN: Howard, just one quick follow-up.

Yeah, just a very quick one-sentence comment. It would be nice if when they were up there they could be the kind of thing, which could be replicable, so people could independently run similar tests.

MR. YONKERS: Okay.

MR. BEALES: Joanne McNabb.

MS. McNABB: Thanks, Steve.

You mentioned that you would be using additional mitigation strategies to further protect privacy even with the newer model. Can you describe what's on those, would be?

MR. YONKERS: Yeah. In fact, one of the first things I think it starts with is training and education itself. And one of our transparency is making sure that the user, the person who is actually the holder of the document, actually know exactly what they have and what they can and should be doing to make sure it's properly protected. Everything from, you know, just don't hand it over to someone else because they'd like to see it.

You know, don't make it easy for someone to try and scan or read the RFID tag. That, you know, there is some personal responsibility involved in this as well, just as when you're at the port of entry, you have to probably present your documents, I think part of this is also an education, not just a campaign, but just good information, Q&As, helping people understand what will make that difference.

But there's other layers of technologies that can be added. There's things where you can randomize the ID number. There is low-level encryption and there is high encryption. There is a variety of things that are available, each coming with their own price of course and some of those prices meaning a detraction to accomplishing the mission. Other things just very expensive. But other things you can readily add.

One of the things that we've looked at is something called a Faraday cage which could be just a nice slim sleeve that's metallic and you could put the I-94 in that. It would be unreadable. You would not be able to read the document in that Faraday cage. We know that's already been established with the passports. It's built into the cover.

Now I'm not saying that we necessarily want to have something that could be lost or discarded or forgotten. So, you know, that's one of the first things we're looking at, but the technologies continually improves. And a I like is being, you know, a partially a driver of this new technology as part of the federal government, is this allows us to help to not just making the technology work better but making sure the technology is going to provide the privacy and security safeguards that we expect.

And so even if people don't quite understand, 'Well, what is the concern with the RFID tag number being intercepted. I don't understand how you could use that information,' that we could say: Well, it is a concern, and we want to have a mitigating strategy to protect against it. And when you come with your new version of technologies, we want to also see what additional things can you provide that will allow us to keep building the trust with the public.

MS. McNABB: And did your study show -- I've slipped another one -- did your studies show how much time is saved at entry?

MR. YONKERS: How much time. In terms of -- well, the proof of concept right now is mostly looking at how well can we even read the document and in looking at what types of operational issues are there with reading it and pre-positioning information and that type of thing.

But there were time-and-motion studies. And, you know, I think we looked at a savings of potentially several minutes. It's hard to go out there and say that's what you're going to find in every situation.

In fact, what we've wanted to say really is because we need to really make sure that we're verifying people's identity and their travel documents for every person in every port of entry, that what we really want to do is make sure that we're not creating delays. We want to make sure that we're not slowing down the border processing.

So if we can add this additional functionality, this additional security protections, and not increase wait times, then we've been successful. If we do even more and can actually reduce wait times and truly facilitate travel and trade, then so much the better. But I think the reality is certain port of entries are going to have more impact than others in terms of making the process go faster or better.

MS. McNABB: Thank you.

MR. BEALES: Joe Leo.

MR. LEO: I would like to explore with you a moment the issues of the I-94 and exit, and on the issues of data integrity. And you mentioned privacy in terms of --

MR. YONKERS: Um-hum.

MR. LEO: -- security with data integrity. And so I'm sort of lost a little and I need to help -- you help me get back on the path.

And that is when we looked at the old INS and the old '90 data collection and the manual filling out, --

MR. YONKERS: Right.

MR. LEO: -- we recognized that the CIS data today in and out is really fraught with errors. Let's just leave that as a blanket statement. So one of the things is to create a new system that will, you know, make a vast improvement on integrity of the data.

So I am a little bit at a loss as when you go on the I-94 at 40 miles an hour and you go out of the country and a read rate -- a failure read rate of the reader and I come back. And you say, 'Well, you didn't leave right.'

And I say, 'Oh, yes, I did.' And so there's an error-rate issue here that may be as equal or worse than, or whatever.

And the second point of the redress issue is since there's no identifier, that's why I need for you to help me a little bit --

MR. YONKERS: Um-hum.

MR. LEO: -- on the exit, there's no identifier, I mean how do you connect the individual with the piece of paper or the RFID tag and make a conclusive statement that you didn't leave the country right now and I'm trying to get back in.

And so I need for you to dwell a little bit on our twin goals of this Advisory Committee, which is privacy and integrity of --

MR. YONKERS: Right.

MR. LEO: -- what you're doing. So would you --

MR. YONKERS: Absolutely.

MR. LEO: Would you mind addressing that for me for a few minutes?

MR. YONKERS: Sure. Well, with the proof of concept, what we should be able to say is a tag left the U.S. We're recording the exit of the tag. Can't say you're recording that that person, individual left. And we realize that right upfront and we knew that from the very beginning. What we first want to see is this technology even going to help us record those exits at all. How well can we actually do this. What is the read failure rate. Those are exactly the types of issues we're looking at with the proof of concept.

And realizing that this has to be an incremental approach, that we have to move actually fairly slowly and methodically as we look at, okay, so if we can accurately read the RFID tags at speed as they are being exited, okay, now then how do we associate it with the person. Well, you could just start associated with the vehicle.

We already do license plate readers for entry. That might be another way to increase the association, but I think Jim Williams has often said that really you want to have some type of biometric association. You want to be able to have something linked to the RFID tag itself that says it's Steve Yonkers that has left so that for data integrity purposes we could feel pretty rest assured that Steve Yonkers left the country and not just the tag.

Now currently when people leave we don't really know when they left, and if they come back the next day we can reasonably be sure they left the day before. But when people leave and come back months later, the current process is we just don't know how long they stayed. Very difficult to confirm whether they stay or not.

The incremental part of this is giving us just a little bit more information. The critical part, though, is compliance aspect. As of right now when you're saying, 'Well, we think the person left but we're not sure,' we're not going to use that information then to say, 'Well, we're going to refuse you admission, because we didn't capture the exit.'

The same way we're doing the exit testing right now for the airports and a couple seaports, which is for those people departing from those airports and seaports, they must biometrically exit. It's a mandatory requirement, but we know we're in a testing phase, which is why when someone comes back into the country, if you forget to go through the process or if there was a problem, it's not being held against you, it's not going to impact your ability to re-enter the United States, because we're looking at a testing scenario.

I think it's the same thing with the land border, which is -- now is not the time that we're going to start seeing, 'Oh, we're going to hold you accountable because of the information in the database when we know that we can't be reasonably assured that we can properly associate you with that tag,' no, that will come. The technology to get us there is probably coming, but it's not here yet. And when that time comes, then that's when you build it in and say, 'Okay, we can be reasonably assured you left and if you haven't left and we're probably going to ask you some additional questions.' But CBP officers are going to know to what degree they can really rely on that information, as we move towards incremental stages. So it's very much a work in progress, but for us it's very important to know now how well is this technology going to work for us currently and can we keep building upon success of this proof of concept.

MR. BEALES: All right. Ramon, you again get the last question.

MR. BARQUIN: I know that we're not the only country that's been experimenting with this technology in the entry-exit process. I believe Australia, New Zealand, and Singapore -- have we looked at those experiences and are there any lessons learned that we can apply?

MR. YONKERS: I know that our mission operations and implementation management people have worked and talked to the other countries and tried to explore the lessons learned and the best practices that they're applying. From the Privacy Team perspective, I can't say that we have looked at their technologies or even attempted to assess what privacy concerns and operational connectors they have. Our team is really just focused on the application we're using for US-VISIT. But we definitely try to avail ourselves to what others are doing in the same area and particularly in the area of trying to make sure that we're using established best practices.

MR. BEALES: Thank you, Steve. We really appreciate your being here.

We have a here slight scheduling difficulty here. And, Charles, if I could ask: How long do you need and should we do that before lunch or after?

MR. PALMER: Before.

MR. BEALES: Okay. Then I think what we will do is move the Framework Committee to after lunch and let Charles give the Report from the Emerging Application and Technology Subcommittee, and then we'll get to eat, so thank you.

SUBCOMMITTEE REPORT: EMERGING APPLICATION AND TECHNOLOGY

MR. PALMER: Thank you, Mr. Chairman and thank you, Steve, who's already escaped, for visiting with us yesterday and again today.

I just wanted to make a few comments about our Subcommittee. The Emerging Applications and Technologies Subcommittee, the EAT Subcommittee. Our goals is to delve into data privacy and integrity aspects of emerging technologies that are being or may be deployed by various components of DHS.

And for each one of those studies we have two real goals. We hope to enter into a dialogue with the organization that is involved, to discuss and understand what problems they might address with this emerging or new technology or application, and how they're considering on actually using it. This needs to be a dialogue. It needs to be both directions. And that's our first goal.

Our second goal is to be able to provide feedback from our perspective as perhaps in some cases domain experts, people who write books and so on, about the potential data privacy and integrity impact from our perspective, which may very well be different and perhaps less informed than that of the persons we are speaking with. But we are here to make those kinds of comments and assessments and provide the advice.

Our aim of course is not to con anybody. We're not here to criticize a particular program. We're not here to chew up and spit out an initiative that's been proposed, or anything like that. But we want to look at the bigger picture. This is, in particular, the topic we just discussed. It is one of the first uses of RFID and that it is actually touching the public this broadly or potentially this broadly.

So clearly we're interested in this particular program, but we are specifically interested in the broader issues around using RFID to track, monitor, watch -- whatever word you'd like to use -- humans.

In some cases we may be talking with an organization or a component that is already deploying technology, in which case our response time would have to be much quicker and perhaps maybe not nearly as gentle as you might hope because we're in a hurry and we have to get our feedback back in a hurry.

Now as many of you know and has already been intimated earlier, we released a report, a draft report. I want to make sure everybody understands. This was a draft report on the use of RFID technology for human identification.

As such, the draft represents work of the Subcommittee, a work in progress. It is not the work of the whole Committee. It is not the work or result of DHS, the Privacy Office, or anybody else. It is not a completed work. It is a draft.

It's also important to note that the draft is not meant to be an exhaustive study and comparison of the widest possible combination of RFID technologies and their data privacy -- data privacy and integrity impacts. It is not meant to be an exhaustive study.

Thank you.

There is indeed a multitude of beneficial uses of RFID. Nobody will argue with that, either on the Subcommittee or in the public. It's also true that many times with technology, a single term is adopted to reference or represent a multitude of technologies that may very well still be evolving. I mean as Steve said himself, we are hoping for newer, better, cooler technologies to come that may make things easier.

At the same time there are some uses of RFID technologies where the benefit that they offer is still a topic of thoughtful debate. And for those particular uses, the benefits may not outweigh the data privacy and integrity concerns.

As the result of releasing our draft we received quite a few comments from the industry, from the public, from nonprofits, from DHS itself, and from others, Members of the full Committee. And we appreciate each and every one of them. They varied from -- well, these comments are available for your review, if you wish. I believe there's copies on the back table outside somewhere.

The comments varied quite a bit, ranging from, "You guys didn't get the definitions right" -- perhaps. Some suggested we focus less on specific technologies -- I mean specific applications of the technology and more broadly focus. Good idea.

Some highlighted the benefits for security and antifraud, not really paying -- not highlighting the privacy and data-integrity aspects but thinking more of the positive aspects. And that was helpful as well.

And of course some comments came from the RFID industry itself, touting the benefits that newer technology and, in some cases, "Ours is ways better than that" kinds of comments, which were very enlightening in numerous cases.

And of course there were a good number of comments that refused to consider the use of RFID technology for anything. That was not really so good for people and might not be good for anything in particular.

So you're going to expect that kind of a range of comments, and we appreciate each every one.

So in addition to listening and studying these comments we met with US-VISIT folks twice since the draft paper was released. They have provided us with answers and expansions of information that we had already received. And they are agreeing to continue the dialogue because we still have many unanswered questions and concerns we'd like to discuss with them.

We would also like to reopen our discussions with the Customs and Border Patrol [sic] component of DHS, as well as any other component within DHS considering the use of such technology for the identification of humans.

We will be of course studying all these comments and meetings and discussions we're going to have. We will be updated our draft and be producing another draft for further comments before the next Committee meeting in September.

The -- one last comment. The official commentary period has ended, but I am going to ask the Committee to reopen -- or the Office to reopen the comments path. And if that can't happen quickly, the email address is indeed on the website, and just send them on over there, and we will get them.

So I encourage you to, please, share your knowledge and expertise with us. We -- I have some amazing people on this Subcommittee, some of whom may wish to add their comments now. But every piece of information is helpful. Every piece of information can make it all better. So thank you very much.

MR. BEALES: Thank you, Charles. I think we can reopen the comment period without difficulty. And anybody who has anything more to say or any more information that might be useful to the Committee and the Subcommittee, please, by all means, send us an email and tell us about it. And we are -- we are very interested in that.

I want to thank you, Charles, and the Subcommittee for your work on this draft. There is a lot of expertise around this table, but any time we tackle a particular issue there's also a learning process that we all go through. I think you've given the rest of the Committee a great start for thinking about this issue and, you know, the issues that it raises; and that we're engaged in a productive process that will lead us to hopefully useful recommendations about the role of our RFID. But it is a learning process and one that will continue.

Is your tag up, Joanne, or...?

MS. McNABB: No.

MR. BEALES: No, okay.

All right. Are there any other questions, comments from the Committee?

All right. Then thank you. We stand adjourned for lunch. We will resume on time at one o'clock. (Luncheon recess)