Department of Homeland Security
Data Privacy and Integrity Advisory Committee

OFFICIAL MEETING MINUTES

Wednesday, September 28, 2005
Hotel Bellwether
One Bellwether Way
Bellingham, Washington 98225

MORNING SESSION

MR. ROSENZWEIG: Good morning. My name is Paul Rosenzweig. I am the chairman of the Department of Homeland Security Data Privacy and Integrity Advisory Committee. I want to welcome all of the public, as well as our speakers to this our third meeting of this Committee. I think I'm comfortable in speaking for everybody in saying this view out from the back certainly is the most beautiful place we've been so far, and we're very fortunate to be here in Bellingham.

A few announcements and administrative matters and news such as it may be.

At its administrative meeting yesterday, the Committee adopted the bylaws, which are in draft form in your packets, and with one amendment to section 4-B, 3-A. 4-B 3-A reported to require the taking of names of all those in attendance, including the members of the public. We, being a privacy Committee, recognize that that was an unnecessary information request and have stricken from our bylaws. The bylaws were proposed based upon perceived legal requirements, and they may intervene, but they're not part of our bylaws, so you may treat the draft that you got as our final.

The other thing that the Committee did at its administrative meeting yesterday is approve the concept proposal that is in your packets. We have agreed, in principal, to work with another federal advisory Committee, the information security and privacy advisory board which reports to the National Institute for Standards and Technology and the Office of Management and Budget. They too have a brief to discuss, to consider issues of computer security and privacy, and the two Federal Advisory Committees have decided to join forces for a long term project to develop a framework for thinking about privacy in the new information age. You might call it Privacy, the 21st Century, something like that.

We intend to establish joint working groups and step back from the current status of the law and examine what new policies and legal requirements ought to be put in place or adopted. We intend to have several public meetings of the joint working group over the course of the next six to twelve months and develop a much more definite scope of work in terms of reference. But that seemed a relatively momentous note.

I want to make one other administrative announcement. At our meeting in Boston, we had testimony from a large number of very able witnesses, and we asked a series of follow-up questions to them, which will continue to be our practice here. Since we have no powers of subpoena or demands, if people don't answer us, the only thing I can do is make that fact known, transparency being an important privacy value as well in some instances. So we have yet to receive answers from three DHS components. Two are in the process of clearance for us, so that's satisfactory. But I wanted to place on the record our disappointment that we have yet to hear from the Homeland Security Operations Center in respect to the questions we've asked, and we're going to try and get those answers for us and for the public as we go forward. Hopefully mentioning that here will advance the process some.

Those are my administrative announcements.

Our first witness today is Nuala O'Connor Kelly. We've made it a practice in the Committee to hear at the outset of each of our meetings from the Chief Privacy Officer for an update on generally what is happening within the Department, and I gather that this will be something in the nature of a final delivery. So, Nuala, the floor is yours.

MS. O'CONNOR KELLY: Thank you, Paul. Thank you, members of the Committee. I'm grateful to be here to speak with you again. I am pleased to report on our office's progress since we last met. First I want to start looking after two additional hires at the headquarters level: Erica Perel, who is our new counsel, working under our chief counsel for privacy; and Billy Spears, our new director of education and training. We are delighted to have them on board as well a number of additional personnel contract staff, our new director of outreach, and some other extreme players. And of course we are grateful to Becky and Tamara, the two that put this meeting together. Great personal time and effort.

We have had a number of major events in the Privacy Office in the last few weeks, in fact. Most recently I'd like to start with our Joint Review of the Passenger Name Record Agreement with the European Union. We completed a successful review with the delegation from the European Union a few weeks ago. We did two and a half days of site visits and in-depth briefings from the Customs and Border Protection Division, the

Department of Homeland Security on the compliance agreement that was signed in May of 2004, which required strict adherence to a number of policies, but all in particular the close keeping and safeguarding of personal data and the expulsion of sensitive data which has been accomplished both manually and also electronically at this point. A report from the office, I think, is available in your books and it's also available on the Privacy Office website. I'm very, very pleased at the work that was done not only by our team -- again, Maureen Cooney, which is our senior international advisor; John Kroft, our director of international privacy programs; and Becky Richards, our director of compliance working on that audit investigation. I'm very delighted that that is concluded, and we got very high marks from our European counterparts.

Also recently the Department and our Office sponsored a workshop on the commercial data by the Department of Homeland Security and the Federal government within and outside the government for a number of days to discuss whether and how and why commercial data might be used in Homeland Security efforts. I think it was a fruitful kind of formal discussion of the same issues we're dealing with inside the Department and working with in the policy community on a daily basis.

The office has a number of pending reports, and I hope to be able to report they are out of internal clearance when we meet again in December, as well as we are working on our annual report, which should be out hopefully sometime in the end of next quarter, and, again, we will report to Congress on the progress in the office and about the concerns of privacy issues at the Department.

Other issues to cover today. I think those are most of the administrative issues. And let me give you a brief update on the office, for the folks who are sitting behind me who may not be familiar with it.

The Privacy Office, as you all know was created by statute by the Department of Homeland Security in 2002. We are now at headquarters and 30 strong, and we supervise the work of over 400 privacy act, freedom of information act, and privacy officers in the Department of Homeland Security.

I was originally going through some files, and I found my list of three things that I wanted to accomplish when I was appointed to the job in the first three weeks of the Department's creation. And they were setting up a sound infrastructure and sound office for continuity of the issues, working with our international partners for recognition of our privacy structure, as well as incorporating concerns of other countries about their offices' data, and also to develop some rules for work with the private sector, and particularly in the use of commercial data. And I think we have seen great accomplishments.

Let me go in order. I think I can say that we are tremendously proud of the structure we have created at the Department of Homeland Security with technologists, specialists, educational training people, compliance folks as well as lawyers in a multidisciplinary approach to privacy that is embedded in the Department and very effective and in a very lasting way. I think our international efforts are tremendously valuable. We were the first office to be given official observer status at the International Association of Privacy and Data Commissioners just a few weeks ago in Montreux, Switzerland. And that is the second time this office has been granted such status, and I give a tremendous amount of credit to Maureen Cooney for her work on that issue as well as assisted by John Kroft.

And last, I think we have moved forward in the debate in the conversation about the intersection between the commercial private sector and public sector in the use of personal data for Homeland Security in counter-terrorism efforts. And so with that, I think you all know what I'm going to say next, which is: This week is my last week at Homeland Security. And I have been most honored to serve all of you citizens of this country and to serve with my fellow staff at the Department. And it has been a tremendous honor to serve the country since 2001. I have now served under four different Secretaries, all of whom have been tremendously supportive of my work on those issues, Secretary Don Evans, Andrew Vaughn (phonetic), Tom Ridge, and now Michael Chertoff. But it is time to go back to the private sector.

A number of you asked me questions, and I think I need to say on the record the answers to them. I was not asked to leave. No one suggested that I leave. In fact, the Secretary just a few weeks ago told me how much he wished I would stay. The job has not become more difficult under the new Secretary. The job has always been difficult, so it's no more difficult than it ever has been.

The departure is on my own choosing. I have been afforded some opportunities in the private sector that I simply cannot say no to. But most of all, I need to reiterate with Tom Ridge, which is: Public service is a family thing. My husband and my child have suffered a great deal. I am very proud of the work I have done. So thank you.

ATTENDEES: (Applause.)

MR. ROSENZWEIG: Thank you very much, Nuala. I'm sure that as you leave there will be many who will reflect upon the accomplishments of your office, as it developed from basically ground zero to where it is now, and we'll have many positive things to say.

I think for our own part on the Committee what is most notable is the willingness of the Department and of your office to create this independent body, over which you have relatively little control. And to people with very strong and independent-minded folks who are happy -- perhaps more happy than you'd like to give you their advice and counsel, to tell you when they think you're right but also when they think you're wrong, and it is, I think, a notable achievement of the strength of the Department and of your office to some confidence that you have a net for humility that comes out of that to create a group such as this. And since you are our sponsor, we will look forward to a new sponsor sometime soon, but thank you for the initiative in creating this body, which I think we all very much appreciate.

MS. O'CONNOR KELLY: Thank you. And I just want to say, now that I've composed myself a little bit, that the Committee indeed is the creation of this office, and we are tremendously proud and grateful for all of your service.

I do hope that the Committee will continue to be an advocate for the position of the Office of Chief Privacy Officer, not only at this Department but at other federal government services as well.

But it is true, Paul, the Committee is not just an extension of the Privacy Office. It is an able-bodied critic when appropriate and, hopefully, an outside voice. It is yet another formal structure which I think gives voice to the incredibly important conversation about how our efforts to fight the war on terror and make our country safer impinge upon our personal space. And I wish you good luck and Godspeed in that effort.

MR. ROSENZWEIG: Thanks very much, Nuala. We look forward to maybe seeing you at our next meeting in a private capacity.

Our next witness is Mr. Trevor Shaw.

MS. SOTTO: MR. Shaw is the Director General of the Audit and Review branch of the Office of the Privacy Commissioner of Canada. He is a chartered accountant and certified management consultant by professional training, and for 25 years,

MR. Shaw has been auditing Canadian government departments and agencies at both the federal and provincial levels.

Mr. Shaw's favorite quote is Winston Churchill's, "The worst form of government is democracy, save for all the rest." So here we are letting our cherished democracy work at its finest. Thank you very much, Mr. Shaw, for joining us.

MR. SHAW: It's indeed a pleasure to be here. First time in Bellingham. Beautiful spot. And I bring you greetings from Jennifer Stoddart, the Privacy Commissioner of Canada. She would've been here this morning, but her change in venue complicated her existing travel plans, so I got the call last Thursday that said that, "Trevor, I need you to fill in for me." So I guess I'm pinch hitting, I guess, is the phrase.

And certainly Heather Black, the Assistant Commissioner, and Raymond D'Aoust, the other Assistant Commissioner and Province Commissioner of Canada send their greetings.

Indeed this is actually an opportunity for us to actually look at ourselves because just hearing the pieces of information just in the last five minutes or so tells me that there may be some comfort that Canadians can take in the form of this structure and the operations of Privacy Commissioner of Homeland Security is actually in place and working, because there are apprehensions on the other side of the border. So hopefully from the information gathered from this, I can include it in our next annual report to parliament so they're aware of this structures overseeing privacy. So thank you for the opportunity.

Now the set of context for my remarks -- and I never prepared a text, but what I'm about to say to you is what Jennifer Stoddart would say to you should she be here. So I guess she's here in spirit and definitely with great interest to the matters of international perspectives on privacy and security.

Now, for those of you not familiar with the Privacy Commission of Canada, I thought we could spend just a few minutes with a quick overview.

The Privacy Commission of Canada is an agent of Parliament who reports directly to the House of Commons in the Senate. The Commission is an Office who fulfills an oversight role and is independent of the government. We don't take instructions from them, etcetera. We are completely independent. Well, we are dependent on them for resources, of course.

Our mission is to protect and promote the privacy rights of individuals, and we observe the application of Canada's two federal privacy laws, the Privacy Act and also the Personal Information Protection and Electronic Documents Act, known as PIPEDA, although some would say PIPEDA (pronouncing). I can't figure out whether it's PIPEDA or PIPEDA (pronouncing), but it works either way. The Privacy Act, of course, applies to the public sector, if you will, the operation of different Departments with the Agency and PIPEDA applies to the private sector.

Now, this sets the scope of oversight and responsibility for some 160 Federal Departments and Agencies and Crown corporations under the Privacy Act, as well as the countless tens of thousands in private sector corporations, commercial operations in Canada that are subject to PIPEDA.

We are an advocate of the privacy rights of Canadians that empowers us to do certain many things: investigate complaints and conduct audits under two Federal laws, publish information about personal information handling practices in the public and private sector. We can conduct research into privacy issues so as to inform the Parliament and public, and indeed to promote understanding of privacy issues by the public. And we can review and comment on privacy impact assessments completed by Federal Departments and Agencies.

Our particular power, if you will, is provided under the administrative policy of the Church and Board of Canada where every Federal Department and Agency is required to conduct what we call PIAs, privacy impact assessments, for any new system development there is.

This indeed is a window unto us of what actually happens before things happen. It's a positive control where we can actually bring privacy issues to light and ensure particular risks to privacy or address them and develop any new system or operation introduced by Federal Departments.

It's one of those things that takes place behind the scenes that people aren't really aware of, but we do make a difference. We have commented on things under development by the RCMP, CC, etcetera, through each privacy impact assessment.

Now to the heart of the matter on this matter of national security. None of us here doubts certainly not the seriousness of the national security issue and our depth of concern on the citizens in western countries about being struck by terrorism. Now, Canada you may perceive as a relatively peaceful country, which it is, but we have actually had terrorist activity and acts in our country. Not many, but when they did, they certainly shook us up tremendously. In 1985, for example, you may recall the flight that originated in Toronto, Canada which flew over the Atlantic and killed 329 people aboard. About the same time, there were some ordinances on a flight from Vancouver to Tokyo that wound up exploding in Tokyo, killing two baggage handlers. Only by luck and circumstance did it avoid killing all passengers on the plane.

Canadians, as a perspective, generally see it as an essential duty of government to ensure their security. At the same time, they see government as guardians of fundamental values. One of those fundamental values is privacy, and, therefore, they look to us to act in that capacity.

This, as you probably are already quite aware, sets such an interesting challenge or tension between the matter of security, on one hand, and, on the other hand, ensuring privacy and protection of personal information. Certainly I don't think in the sense of history the development of our approaches of user privacy has come through the British system, etcetera, but I don't think -- We are not going to go to the length that, as somebody put it, in 1775, that your Patrick Henry in a slightly different comment said, "Give me liberty or give me death." But surely you can see the importance of preserving fundamental rights, even in the face of egregious threats to our society and, indeed, to our security. Like the rest of you here today, we recognize the need for state intelligence apparatus. The Privacy Commissioner of Canada, like other Canadians, recognizes the collegial responsibility. In this regard, the democratic congress share to prevent themselves from in fact becoming conduits for terrorism. Therefore, cooperation, exchange of information, all of those things are really important. Still, attention to security issues does not mean, as Jennifer would say, burying their heads in the sand when it comes to matters of privacy and consequences. In this regard, generally speaking, we think there's a need to flex the muscles of accountability and transparency to ensure that agencies to which we entrust powers do not interfere more than absolutely necessary with this fundamental right. We must have the means to ensure power is exercised responsibly and deliberately and, in turn, maintain this notion of proportionality. Indeed when we review the PIAs, is the surrender of privacy proportional to the specific need that needs to be achieved through the change to an improved security? Now, as an auditor, we can do that in various different ways. One of the important mechanisms is, in fact, audit, we call it compliance reviews sometimes, to actually see what's going on. We're trying to beef up our audit capacity in the privacy audits to submission of treasury board so we can do this more extensively and more effectively.

So as an auditor, I have been picking up things as I'm learning from the U.S., and one of the things I've found just recently that was brought to my attention is, this could just be, in fact, the report of the Justice Inspector General audit division that recorded this August on the review of Terrorist Screening Center efforts to support the Secure Flight program. That's useful information for us as well. It's also comforting that such reviews are indeed going on. There was also a report recently released on probably the -- There's a Secure Flight Working Group that produced a report just recently, just a matter of a couple of weeks ago, on the Transportation Security Administration. It's something I haven't read yet, but I certainly will be to see what I can learn and understand from them.

Now, the Office of Privacy has watched with increasing concern as the events of September 2001 calls for ever-increasing powers of intrusion in the name of fighting terrorism and protecting national security. We are appropriately cautious about the cost of transnational or continental integration approaches to information gathering and intelligence sharing.

We are kind of uneasy with the private sector also being co-opted or brought into or pulled into the security apparatus of the state. I happen to know through one of the little press releases that apparently your Transportation Administration indicates it will not be doing this, although there's some uncertainty whether that's going to be permanent or just simply temporary.

Now, certainly it's not an easy time for our office, and that is responsible for protecting the privacy rights of Canadians. It's not easy when we remember the citizens of various western democracies to not look at this important light through the same lens. The weight they attach to this privacy varies considerably and reflects the histories of these democracies. Now, when somebody said to me, "You're going to try to do a talk on international perspectives on privacy," of course the first question I asked was, "Is there some kind of definitive study somehow or something that would actually allow us to understand the different regimes of privacy at work in North America and in other countries of the world?" I haven't found one. And when I hear the chair mention this sort of stepping back to look at the overall privacy measures in the framework of the structure of the United States, this is indeed a challenge.

And actually put the information to compare the different ways of approaching privacy in our hands, I hope it will be considerably easier. I don't know who would do it or who would pay for it, but it would certainly be quite an exercise. Certainly looking at other countries, their perceptions of privacy, particularly in Europe, and for those countries that have suffered under the hand of totalitarian leaders and totalitarian states, their look at privacy varies strongly.

One of the things I've learned personally, and it's certainly a perspective on my part, is to understand fundamentally that in a democracy government is openly transparent, and the lives of citizens are kept private. In the totalitarian states, it's the opposite. The government is secret, and the lives of people are completely open and bare. I didn't really realize the significance of the job I undertook until somebody -- after reading things, I'm able to appreciate what that really meant.

Now, when we look at basic -- I think between Canada and the United States, our interest in sustaining privacy and protecting basic democratic values are the same. But when it comes to privacy, our approaches simply seem to be quite different; that is, the system structures and approaches to doing that. In other words, in the United States, if you'll permit a broad generalization, it seems that it's tended towards several what are called sectoral approaches, and sometimes specific response s to particular conditions or events take place. In Canada, on the other hand, it's more of a comprehensive approach. Canada and its European neighbors have been able to adopt more comprehensive privacy laws.

It was sometime ago when I read something that said that in the United States, there may be as much as a total of 3,000 privacy revision laws at the federal and the state levels. In Canada, I think there might be five: two basic federal ones and three in BC, Alberta, and Quebec. And Ontario has a -- we recently introduced the Health Information Protection Act. Now, perhaps there's a small example to explain the difference or to highlight this basic approach. In the United States, I understand you have something called the Video Privacy Protection Act of 1988, and some of you may recall or remember that back when it took place, after the Germans caught hold of some sensitive information about a supreme court nominee, Robert Bork, who, let's say, amended some videos that were kind of embarrassing. So that one was introduced to prevent anyone from disclosing the title videos a person may have to rent or buy. In Canada, of course, we have no such comparable law in specific. However, under our PIPEDA, or PIPEDA (pronouncing), the principles of lawness and comprehensiveness enacted, in fact, prevent or not allow that by the application of principles associated with the act. So -- Now, PIPEDA applies federally in Canada to everyone operating -- commercial operations in Canada, except in those jurisdictions where it deems a similar statute, similar legislation, which is, as I said, earlier was British Columbia, Alberta, and Quebec. It also applies to the provincial transport or flow of information between entities; so in other words, in federal sense.

Generally speaking, there seems to be a greater tolerance for the use of personal information for commercial purposes than in Canada. Perhaps it goes back to one of your turning events in your history when President Coolidge in 1925 said "The chief business of the American people is business." Now, in Canada, it seems we're a little bit more cautious, if you will, or sensitive to the use of personal information in commercial operations.

Certainly in the United States it seems that personal information is a commercial commodity, and indeed it's a very valuable one. Just look up the data mining operations that have emerged over the last decade to realize just how valuable personal information is as an asset and a minority of that market. In Canada, it is generally less tolerant in the use of their personal information. So it's little wonder, then, when Canadians see major data breaches that occurred in ChoicePoint and Lexus Nexus. Getting a little worried. And I think it raises the question about what information about Canadians was inadvertently or criminally disclosed, breached, whatever you want to call it.

So this, in turn, raises the question: What would a Canadian do in the event there was some personal information that leaked in one of these data leaks that impacted them directly, etcetera, and what are the protocols, methods in which they can be addressed? And, indeed, I don't even know if a Canadian has the right to be notified of a breach of personal information that could affect them.

Just finding out, for an example, whether how many Canadians would have been impacted by the breach, how do we find that out, if we're protected or not? As far as we understand it, there would have been Canadians impacted by such a breach. Now, the basic point is, I think, that even though we have a similar -- We are indeed one of the strongest trading partners in the world, and we share a lot of commercial space. The commercial bonds are strong, and in terms of shared concern of terror, we handle personal data quite different and we probably see it differently.

Now, the whole idea of our concern about privacy does not impede a legitimate disclosure of personal information for purposes relating to national security of law enforcement investigations. Indeed, Canada's privacy laws allow for this law exemption, release of personal information for law, and other matters affecting the security of Canada and its allies, but we don't blindly accept calls for greater access to personal information for means of national security purposes.

And, in particular, Canadians are becoming more aware and concerned about the transfer of their personal information across borders, particularly when there's access by foreign governments to that information. Now, that concern is brought out by a survey that we did in responses by the National Survey of Canadians about emerging privacy issues. There was a pervasive belief, a perception among those surveyed, that personal information is flowing freely to other countries, particularly the United States, and going to other countries as well. This belief is particularly true in relation to companies transferring personal information about customers from companies outside Canada. The majority of Canadians believe that personal information held by governments is also flowing across borders.

Now, the problem is, what information is made available to Canadians, parliament to know with some certainty what information is flowing, under what circumstances, for what purpose, and what are the controls surrounding that information. Absent information to inform instructively, accurately, and reliably may, in fact, feed a perception that it's worse or out of control. It's an interesting dynamic. We're trying to do something about that. Now, that survey found the level of concern that goes to transported fellows of personal information is extremely high. Only about one in ten Canadians expressed a low concern in the event that Canadians' personal information was to be transferred across borders. The concern is somewhat lower if the transfer of personal information relates to international security, but the concern remains generally high for any activity, regardless of the purpose or its rationale.

Now, this survey, actually, has found a complacence with the outsourcing of data processing, for example. In fact, the department that was looking to outsource its data collection did a consensus survey. And there was some concern that the information would reside by the contract, the personal information would be held by a contractor outside of Canada. And when that became known, there was quite a public reaction to that, and, in fact, it stopped it.

Under the newer arrangements, that information will, in fact, be retained in Canada by the department, and the company who won the contract will simply serve as a way of developing the system, monitoring, and controlling the information itself and will not leave Canada. Basically speaking, when you see that, they tend to not want the reasonably strong protection for their personal information in Canada to disappear as soon as the personal information crosses a border.

Now, the second sign of this concern about transport of data flows was -- of course, you may be aware of the work that was done by David Loukidelis, the practicing Commissioner for the province of British Columbia, when he looked at the implications and consequences of the changes to the Foreign Intelligence Surveillance Act introduced by the U.S. Patriot Act.

Now, in response to that, when he put this out and he sent it -- And if none of you have seen this report, I certainly commend it to you. He received hundreds of briefs from individual Canadians, responses from Canadians, a degree of public participation in the policy that is very unusual in Canada. I don't know if you've -- the engagement in democratic persons, but Canadians, you have to really get tier attention. And what they do is downright serious, and it is, in fact, at the roots. And this one did trigger a nerve.

What works in this review is an awareness of extremely limited protection of personal information about Canadians in the hands of foreign governments, including that in the United States. So in response, in October of 2004, that province passed legislation to amend the Freedom of Information and Protection of Privacy Act to prevent the public bodies and their contractors from storing information, personal information, outside of Canada and/or restrict the disclosure of personal information or organizations from other countries. So this whole business of transport or flow of information is a matter we continue to consider for sure.

Now, you may think that -- and you may say, "Well, why worry about this? It this an attempt to create a storm in a teapot?" After all, Canada and the United States are two of the world's strongest allies, and, indeed, we are bound by many common things, not to mention the longest border in the world. But basically, Canadians and American citizens -- I don't know -- have a great apprehension -- in other words, fear -- very leery of the might of the U.S. intelligence apparatus. They don't want to see their privacy protections that they have called for and supported in Canada vanish as soon as that information crosses some border.

Basically, Canadians want not only to be informed of the transfer of personal information outside of the country, they also first want to give their permission. Now, if that's the case, how do you do that? How do you do that and not compromise or, say, in the process, tip off the enemy? This matter of gaining permission -- opting in, if you will -- this opting in and opting out business, it gets complicated.

You may have heard as a case in point that is really bringing to fore and emphasizing, perhaps galvanizing, this concern about personal information being used in the realm of intelligence and national security. I don't know if you've heard of the Maher Arar case in Canada. He was a software engineer, working and living in Ottawa. He was a Canadian citizen with a Canadian passport. He happened to be born in Syria. But on a stopover in New York, as he was returning to Canada from vacationing to Tunisia in September of 2002, U.S. officials detained Mr. Arar, claiming that he had links to Al-Qaeda, and he was deported to Syria, even though he was a Canadian citizen and was carrying a Canadian passport. He was allowed to return to Canada more than a year later. Mr. Arar claimed that he was tortured in Syria and that U.S. officials that sent him to Syria knew that torture was practiced there.

A basic issue is whether Canadian government agencies inappropriately provided information about Mr. Arar to U.S. agencies and whether this led to intolerable consequence, deportation to a country known to practice torture. There is currently, as you're probably aware, a commission inquiry going on under Supreme Court Judge O'Connor, and we have been watching and tracking what goes on in that hearing. That report of our commission is expected in about a month or so. We will be reading with great interest, and hopefully out of this there will come an understanding of systemic flaws that connect to it and hopefully we can all learn from this experience and strengthen the oversight and controls around this.

You mentioned about the meeting in Montreux -- There was a meeting two weeks ago by the 27th International Conference of the Data Protection and Privacy Commission that was held in Montreux, Switzerland. You may be aware that commissioners from around the globe adopted a declaration aimed at strengthening the universal nature of data protection principles.

The preamble to the declaration recognized the need in a democratic society to efficiently fight terrorism and organized crime. This purpose can be achieved in the best possible way when human rights, and especially human dignity, are respected. Consequently, the press release that accompanied this legislation spoke of a current geopolitical context and, in particular, war on terrorism: the Internet, biometrics, development of invasive technologies, and the appearance of bioducts. These phenomena make it all the more urgent to address the issue of basic rights and freedoms and, in particular, the right to privacy and to uphold these as in viable principles which would be guaranteed in all modern democratic societies.

More to on the ground in Canada, to let you know some of the things we have been doing in the Office of Privacy Commission of Canada in this area. We have been on the ground to help ensure privacy is maintained and its changes in government policy and practice are made in the interest of national security. For example, we provided comment and then a period before parliamentary Committees on Canada's Antiterrorism Act, which has a significant impact on privacy rights. We made 18 recommendations in which we called for checks and balances over extended powers and to ensure transparency and accountability. The core issue was a question of proportionality, as I mentioned earlier, and the apparent lack of any really empirical evidence in studies showing the measures brought in by the Antiterrorism Act are, in fact, necessary and, in fact, work.

We also conveyed an important message contrary to what is sometimes taught when it comes to privacy and security. One notion, we don't believe, is, not always the need to be sacrificed in the interest of the other. Both can be achieved with well-designed law, prudent policy, and effective, but not excessive, oversight.

And on the ground, we're learning through our Canada Board of Services Agency that if you get the personal information management control right, you're also serving security in the process. And that's really important to really understand. And perhaps the Arar case will reveal what actually comes down to something very basic: The information was not accurate, was not complete, was misinterpreted, and so on. Privacy was invaded. If that happened, security wasn't served, while at the same time, data damaging not only an individual but raising great concern over the whole apparatus and perception of Canadians and Europeans.

Another example involves our concern regarding a No Flight list announced by the Canadian government recently. In August we raised concern that such a risk would infringe on privacy rights. We had previously stressed our desires to be made. And what was happening in that process and given the government a list of 24 important, specific questions to consider in the introduction of a No Flight list program. If you're interested in such a list, I have 24 questions and will be happy to provide them to you.

In fact, what had happened the month before, we were wondering -- we had been told we were expecting a PIA on No Flight list, or something like it, and the privacy impact assessment -- that's a part of or present board policy -- we hadn't heard anything, so we just wrote them a letter and said, "What's going on? We're expecting the PIA. This is important," etcetera, "and this is what we think you ought to consider." Well, we got their attention, I guess. And, in fact, what's happened, we've received several briefings since on issue from both Transport Canada and PSETC (phonetic), and we expect to receive privacy impact assessments shortly.

And, finally, we're in the process of conducting a comprehensive audit of the Transborder Information Sharing systems and practices of the newly formed Canada Border Services Agency. Our report is scheduled for early 2006. And my auditors are auditors that have been on the ground right at the border points, seeing what actually happens specifically between at the border, the various intelligence centers, etcetera, etcetera. We are looking at information security, the design of what we call Control of Environmental Sensitive Information Systems.

And you may recall that the Auditor General of Canada had reported about a year ago on concerns about information security on government systems generally. So, again, today we remain deeply concerned about what is happening to privacy in the name of national security, and basically we're saying we shouldn't take things for granted in this civilized society to protect us from abuse. In that sense, we're talking about potential or accidental breaches of privacy.

Some 25 years ago, the Canadian Royal Commission was forced. It was looking at investigation of wrongdoings of Canada's intelligence service, not unlike the commission of today. In some words spoken back then, they are basically mindful for us today. The

Port of Commission spoke of the unique challenge facing the level of democracy and maintaining the security of the state. Those words, written a generation ago, in a different era, nevertheless still ring true today. Put something in the report as stated. The challenge is to secure a democracy against both its internal and external enemies without destroying democracy in the process.

We must be ever so vigilant that our efforts to promote our security do not destroy privacy, one of the essential elements of democracy. If that happens in some way, even in a small measure, then I would ask, "Would the terrorists not have won?" Our office, and myself as an individual, will do whatever we can to make sure the terrorists do not win in any way, shape, or form. I thank you very much for your kind attention. I certainly can answer any questions you may have to the best of my ability. I am not an international expert. I am not a lawyer.

MR. ROSENZWEIG: We have a few minutes for questions. Probably -- in fact, definitely -- not enough for all the members who have already raised their little flags, I'm afraid. It's a crowded schedule. We very much appreciate you coming. For the Committee, I would say first if your statement is in electronic form, our web, our e-mail address is in the agenda and you can send it. And if you would, send as well the 24 questions I added. I noticed we are reviewing the Secure Flight program, here and whatever your 24 questions are, I'm sure our 24 questions are too for our own program. We'll take it from you before you leave. If you have a chance, I would encourage you to stay. You mentioned the Secure Flight Working Group study. The very next witness is from that group. And later today we'll be discussing a paper on the uses of commercial data. So, hopefully that'll -- Those were two issues that were discussed, so I encourage you to join to us. We will take two questions, and they'll be Hoffman and Alhadeff. David, because I saw you first. David.

MR. D. HOFFMAN: Mr. Shaw, thank you for coming and speaking with us today. We greatly appreciate it. If you would provide us just a very quick overview of the process that you have to make sure that the PIAs are filled out, how well that is going, and how you ensure it's followed.

MR. SHAW: We have concern, actually, that PIAs that ought to be done aren't being done. So, in fact, I can't say too much further in this regard. Let's just say we're planning something. The Security Board itself requires that PIAs be done and must be shown to have been done, in particular. There is some concern and Board has actually looked into it and did get indications that there is confusion, perhaps a lack of understanding, of when a PIA should or should not be done, the confusion in particular being definition of data managing and how that applies.

As to the process, under the Treasury policy, departments are required to send the PIA to us for comment and review. We cannot say, "Stop approaching." We don't have the authority to do that. But, however, in the process and under my group, we have PIA officers examining these submissions, and I can tell you that it takes up to a hundred or more hours to effectively assess these PIAs. When the PIA policy was first introduced, the quality of the PIAs were quite poor. This policy has been in place about three, three and a half years. They were quite poor. They weren't well-done. But a result of (indiscernible) are being challenged back, skills acquired, etcetera, that took some time, and the general quality of the PIAs are getting better. So I certainly can send you information on PIA policy, the board policy, in this regard.

MR. D. HOFFMAN: That would be very helpful. Thank you.

MR. SHAW: Thank you.

MR. ALHADEFF: I'll also join the Committee in thanking you for your time and your presentation. I'd like to take you back if possible to the BC report. I've had many conversations with David concerning the report, and one of the things that the report highlights -- and which you highlighted also -- is the kind of concept that the opt-in nature for disclosure to intelligence, my intelligence officials of an investigation is problematic and, in fact, even in Canada, there is a right not to make that disclosure, if seen appropriate for national security purposes, and similar rights exist under the Patriot Act and many other acts and jurisdictions.

I know that Jennifer has engaged in your review of this Act in conversations with the government, and there have been findings of appropriate safeguards that seem to be in place as a result of the X work. Is there a metric or an analysis framework that was used that you might be able to share with us in terms of how that reasonableness finding was discovered? Because it's one of the things that is kind of critical in what we do, is examining what is the justification, how narrow, etcetera. Those are all kinds of factors that we all look at. But it would be very useful to understand if there was an analysis framework that you could share with us on that issue.

MR. SHAW: To be honest with you, I don't know. But certainly I'll try to get back -- And I gather you're talking about the -- Are you talking about what we did on the Antiterrorism Act or --

MR. ALHADEFF: I'm talking about Jennifer's conversations on the Antiterrorist Act, just to kind of debrief David as much as possible on his analysis.

MR. SHAW: Okay. I'll see what I can do in that regard.

MR. ROSENZWEIG: With that, though I'm sure we could go on for hours, I want to thank you for coming. I want to extend our great appreciation to you for taking the time to be here. I want to ask you to convey our thanks as well to the Privacy Commissioner and the other officials in Canada for the cooperative ventures that have gone on between the two countries between the last two years. We very much appreciate your taking the time to be here with us.

MR. SHAW: Thank you. That's very kind of you. And in fact while we're all here, I'm reminded of Woody Allen's quote. "Eighty percent of success is just showing up."

MR. ROSENZWEIG: We will go to our next panel list. This is a surprise witness, for those of you looking at the agenda. It's Anna Slomovic from the Secure Flight Working Group. And, Anna, we're going to introduce you in a second. But if you could keep your own, for the remainder of the witnesses, brief remarks about five, six, seven minutes because I know the members have lots of questions. If I start coughing loudly, that's fine.

MS. SOTTO: Thank you very much for joining us. And we really appreciate your last-minute appearance to talk about a very important issue. Welcome Anna Slomovic.

MS. Slomovic is a senior privacy strategist at SRA International. SRA provides consulting and IT services for federal and U.S. agencies, and in the past year, MS. Slomovic has done privacy work for the Department of Homeland Security Privacy Office and the US-VISIT Program in particular, as well as the United States Department of Health and Human Services. Today she joins us as a member of the Secure Flight Working Group to discuss Secure Flight. Thank you very much.

MS. SLOMOVIC: Thank you. Thank you for giving me an opportunity to talk with you about the report of the Secure Flight Working Group. As you know, the Secure Flight Working Group was chartered under the Aviation Security Advisory Commission of TSA. The group, composed of privacy and security experts from industry and academia was asked to review privacy and security provisions of the Secure Flight program. All the members of the working group were required to go through a security clearance process and to sign nondisclosure agreements.

Our report was presented to ASAC last week. I would like to give you a brief summary of our findings and to spend most of my allotted time answering your questions. The bottom line of our nine months' review of the Secure Flight program is that the program is not ready for implementation because some fundamental questions have not been clearly answered. Because these questions were not answered, it was not possible for us to evaluate the program's privacy and security provisions.

First and foremost, we never got a clear answer about the goal or goals of the Secure Flight program. There are at least four possible sets of goals that we can see. We were told that the Secure Flight program is a matching program that matched the identifying information of those who fly to identifying information of known and suspected terrorists on the government's consolidated watch list. However, a somewhat different goal appeared in the documents that we examined as part of our work.

The draft OMB Exhibit 300 dated February 9, 2005, says that in addition to watch-list matching, violent criminal data vetting has been envisioned for Secure Flight. Such vetting would make Secure Flight more of a general purpose law enforcement tool than a focused terrorist watch-list matching program.

Another possible goal for Secure Flight was taken by Mr. Justin Oberman in his congressional testimony on June 29, 2005. That testimony implies that Secure Flight is headed towards looking for sleeper cells and those who are not on the watch list. I quote from Mr. Oberman's testimony. "It will" -- it, Secure Flight -- "will identify people who are known as suspected terrorists contained in the terrorist screening database, and it ought to be able to identify people who may not be on the watch list. It ought to be able to do that. We are not in the position today to say that it does, but we think it's absolutely critical that it be able to do that. And so we are conducting this test of commercially available data to get at that exact issue." A little bit further down in the testimony Mr. Oberman also said that "That's precisely the reason we have been conducting this commercial data test and why we have extended the testing period and why we are very hopeful the results will prove truthful to us."

Even putting aside the question of whether the goal of looking for sleepers was articulated in TSA's system of records notice and privacy impact assessment for Secure Flight testing, the goal of searching for unknown sleepers is clearly different from a goal of matching passengers to the names on the watch list of known and suspected terrorists.

Finally, TSA was never explicit about the use of Secure Flight as an intelligence tool that permits the government to track the movements of known and suspected terrorists. Because different program goals require different data collection and different analysis, it was not possible for us to address privacy provisions of Secure Flight without knowing what goals the program was trying to accomplish. Furthermore, TSA did not share with us a comprehensive policy document that defines oversight and government's responsibilities for Secure Flight.

Our second major set of questions have to do with the architecture of the program. The Working Group was given very limited information about the program's architecture. We did not learn much about the software and the hardware being used or about how data will be collected, transferred, analyzed, stored, and deleted. TSA did not provide us any test results that showed the effectiveness of algorithms used to match names to the watch list, although a major claim for Secure Flight is that it will improve the accuracy of matching because the program will use much better matching technology than it now uses.

This improvement in matching is claimed to be a sort of compensation for the privacy loss resulting from government collection of personal information of our travelers. Although a system of records notice and PIAs were published for the test phase, we were told that we could not see such documents for the Secure Flight program itself because the documents were still in the rule-making process, and the nature of the rule-making process precluded the disclosure of the documents outside DHS. We did not see privacy policies, security plans, or data management plans for the program.

Third, we did not get information about how Secure Flight is going to interact with other vetting applications running on the same platform. Various documents contain hints that Secure Flight would interact with Registered Traveler and other programs in order to reduce the number of false-positives and possibly in order to make sure that someone on one of the cleared lists doesn't show up on a watch list. However, neither the purposes or the nature of this interaction with programs was ever discussed with us. Given that different vetting programs collect different personal information and operate under different data retention and other policies, we could not determine the privacy impact of these interactions from Secure Flight.

Finally, we did not get any information on the way commercial data sources would be used or see the results of commercial data testing conducted by TSA over the past several months. Because we were provided only limited information, we were not able to do a substantive evaluation of Secure Flight program's privacy and security provisions.

We do have some recommendations, however. Because all the other issues flow from the definition of the program, we recommended in our report that there should be a written statement of the goals of Secure Flight signed by the Secretary of DHS and that the statement should only be changed on the Secretary's order. Even if the program's goals evolve over time, there should be one unambiguous statement of goals at any given time.

Documentation accompanying the statement should include a description of the technology, policy, and philosophies in place to ensure that the system is only used to achieve the stated goals; a schematic to describe exactly what data is collected from what entities and how it flows through the system; rules that describe who has access to the data and under what circumstances; and specific procedures for the destruction of the data.

There should also be assurance that someone who has been appointed with sufficient independence and power to ensure that the system development and subsequent use follow the documented procedures. This concludes my remarks, and I would be happy to take questions.

MR. ROSENZWEIG: Thank you very much. As is our custom, if you have a question, put up your tent thing. Ramon, you were first. And John Sabo, you are next.

MR. BARQUIN: Together with the text of your report, we were also given a statement from Larry Poneman from the Poneman Institute, where in his conclusions he sort of states that he thought that there was an issue of synchronization, of timing, that if the Working Group had been able to see certain reports that had not been produced when you were actually doing your work, that a lot of the questions would have been answered. Are you aware of what reports he's specifically talking about, and then do you concur with that statement?

MS. SLOMOVIC: I have absolutely no idea about Mr. Ponemon's statement. This is the first I have heard that this statement exists. It was not shared with us obviously before it was submitted to TSA. To deal with the substance of the comment, it is entirely possible that there was a timing issue. It is possible that the documents that we wanted to see are further along in the rule-making process than they were at the time. However, we were told repeatedly during a nine-month period that we would have whatever documents we wanted to see, and we asked for documents repeatedly. So, if there was a synchronization problem, I guess my question would be why were we not told these documents did not exist or there was a timing problem or something like that.

MR. ROSENZWEIG: John.

MR. SABO: I think one of the issues was the architecture and the security controls. I'm wondering if the Work Group requested access to a system security plan for the program, or if you know if such a plan exists. And related to that, what degree do you think the security plan or the security controls associated with the program or, you know, their relevance or their insignificance compared to some of the other issues you raised? Are they all roughly the same issue level for the Working Group, or was the security component more significant, you know, in addition to the algorithm and the other issue you've raised?

MS. SLOMOVIC: We did ask for information about program security. We did not receive this information. I do not believe that we were affirmatively told one way or the other about the existence of the security plan, although, under FISMA one would assume that there has to be one. In terms of level of significance, I think it was probably in some ways less significant than some of the privacy issues involved in terms of information, collection, and flow through the system. I think the thinking was that if we could figure out the way the data flows, we would know which security questions to ask.

MS. SOTTO: Thank you, Anna, for joining us. This was a very useful discussion, I think, from you. Could you give us some idea to what extent the privacy officer of TSA was involved in your discussions and in assisting you in procuring the documentation that you requested?

MS. SLOMOVIC: The privacy officer of TSA attended all our meetings. She was part of our e-mail exchange Working Group, the list that all of us shared together. She participated in some of those discussions. She was one of the people who assured us that we would get the documents we need. I'm not sure whether there's more to the question than that.

MS. SOTTO: In your view, is there a need for the privacy officer to have more authority under their particular position?

MS. SLOMOVIC: I'm not sure where the Secure Flight program is now. Maybe it's still in TSA, but there was at some point talk about moving it to a centralized vetting office, so the questions of authority would need to be dependent on where the program actually ends up.

MR. BEALES: Anna, good morning. I really want to thank you for coming. I think your report was a very useful one. We are, as you probably know, looking at Secure Flight. Again, the questions that your group has raised were very helpful to us in structuring our thinking about how to approach the program, because we're still at a fairly early stage. I wanted to ask -- And I agree completely about the importance of being clear about the goals, and the program seems to have had different goals at different points in time, and that is part of what has complicated our thinking about it. But as I understand what the core of the program is – and Mr. Oberman will probably speak to this later -- but as I understand what the core of the program is now, it is to get full name and date of birth information from the airlines from the passenger name records and use that as a government match against the watch list instead of having the airlines use that same information to do the same match with a likely inferior technology. That seems like an improvement. That seems like a sensible concept that obviously there's issues in the implementation that we need to look at, and will, but that seems like a sound and reasonable goal, and I'm wondering what your reaction to that is.

MS. SLOMOVIC: One of the very first things we talked about in our Working Group is the question of whether vetting should be done, whether it should stay with the airlines or come to the government. It took us almost no time to agree that having the vetting done by the government is a better idea than having the terrorist watch list, in any form, go out the various airlines. So the fact that the vetting process was being moved to the government was really not a controversial issue by our group.

The next question is: What information should the government collect in order to perform the matching. The GAO report back in 2003, the report that spoke to the consolidation of all the different watch lists throughout the government, talked about the fact that there were two common elements among all the watch lists, and the common elements were name and date of birth. So it's really not surprising when TSA goes and does tests and compares matching with name only to matching with name and date of birth, matching proofs. That sort of makes a lot of sense.

Our biggest question had to do with the government form of PNR, because PNR data contains no date of birth at the moment, and it contains a lot of other information that does not appear on the watch list and is not itself useful for matching. So the questions we were trying to ask was: First of all, should the government be simply collecting name and date of birth data from the PNR, not pulling the entire PNR. And if they are pulling the entire PNR, should they be filtering things out so as to not get information that is not useful.

We talked about the possibility at one point that the government would not collect the PNR. Last I heard, PNR will be coming into TSA. And it's not, as far as I know, going to be filtered before it arrives. So the question I would ask from a privacy perspective is: Even if it's a good idea to match into the government and a good idea to collect name and date of birth, the question becomes, "What about the rest of the information in the PNR?" You might want to collect some information on what PNR contains. PNR is very drastic from one airline another. Some contain as little as three or four elements. Some contain as many as 50 or 60 elements that will include things like frequent flyer information, special service requests, not to mention seating arrangements and all of that.

MR. BEALES: If I could just follow-up for just a second.

MR. ROSENZWEIG: Yes.

MR. BEALES: Suppose -- And I'm not sure what I think about this, but I'm curious what you think about this. Suppose what the government requires is the basic flight information for pretty obvious reasons, name and date of birth, and the cheapest way for the airlines to provide that information is to dump the whole thing. And let me stipulate that it is not retained, although, obviously, that's an issue. What do you feel about the tradeoff of imposing costs on the airline to keep this information from passing briefly through the government?

MS. SLOMOVIC: There are obviously different ways to do this, right. There's a push system where the airlines would have to invest in a system that would push the data to the government. The different way to do it is a pull system, where the government will go in and pull the data from the airline system. It's essentially less airlines and more global distribution systems and reservation systems. I think you can make a case that flight information and even seating information might be important if there is a match and law enforcement needs to get involved. It kind of would be nice to know where they're supposed to go and what they're supposed to be looking for.

The rest of the PNR information, I think, it's going to be much harder to make a case that the government should have access to it, particularly because the retention period is somewhat questionable. You know, we've heard a lot about the 72-hour retention period. Well, in fact, it's somewhat different than 72 hours because it's 72 hours before flight in order to permit the matching process to take place in an orderly fashion, plus 72 hours at the completion of the itinerary. So if an itinerary is one-day long, then you only add an extra day. If an itinerary is several months long, then the government will retain that data for a very long period of time. That's one of the things we were trying to get at, and the best answer we got is 72 hours before flight and 72 hours after completion of flight.

The other question you might want to ask is whether or not the government has filtering capability to filter out elements that they do not want. It is certainly possible to do that with PNR, and the question is whether Secure Flight should be doing that.

MR. ROSENZWEIG: If I could just interpolate a question, because I thought Howard was going to actually clarify something else. I think I agree with you completely on the uncertainty of the nature of the set of goals that has changed. What I thought Howard was asking was whether or not your Working Group had a consensus on whether or not that core goal, if the program were limited to that core goal of matching names to a watch list, that would be -- whether or not your group thought that was a suitable narrow function and goal or whether you felt that even that was too broad. I mean, that's kind of my amendment to Howard's question.

MR. BEALES: I actually thought she answered that question.

MR. ROSENZWEIG: Oh, okay. Did she say yes or no?

MS. SLOMOVIC: I'm not sure if consensus is quite the right word here, because, obviously, in our group and in the rest of the country there was a lively debate about whether or not the whole notion of an identity-based screening system makes any sense. However, that's not the question we were asked, in part because Congress has already made that decision. They already told TSA they're going to have a matching program that matches names of people who travel to names on the watch list. So, yeah, we had a debate about it, but it's just a personal opinion. I'm not expressing an opinion for the rest of the group. But in my view, that's not the question we were asked.

MR. ROSENZWEIG: Okay.

MR. BEALES: I thought I understood you to say that at least you and maybe the group thought that, given that, that the vetting should be done by the government.

MS. SLOMOVIC: That's right. That's right.

MR. BEALES: Okay.

MR. ALHADEFF: And I'll join the Committee in our thanks for your presentation. I wanted to go to your recommendations, because especially as the recommendations talked about the included documentation, the schematic, and the rules, I was wondering if in the recommendations there was -- and I apologize to the fact that I only had an opportunity to just skim the report at this point -- there was concept of providing some level of guidance because there's a delicate balancing point between when you disclose enough to give people assurance that the system is working properly and has had the correct thought put into it and providing more information that actually allows people through the system as trying to catch the game of the system. So was there any concept of providing some level of guidance as to what the appropriate disclosure is for public purposes versus what the appropriate disclosure is for oversight purposes?

MS. SLOMOVIC: We didn't discuss that explicitly, but I think implicitly there was understanding in the group that providing information that would allow people to game the system is not a good thing. That would kind of defeat the purpose of the entire exercise. We did feel quite strongly, though, that whoever has oversight of the program should have all that information, and one of the reasons we thought all of us had to go through security clearances was we would have access to information which we obviously would not be making public.

MR. ALHADEFF: I guess the follow-up was, in the comments you made around the recommendation, there was the concept that some of this was meant to be publicly available. I guess I was trying to figure out what level you guys were thinking should be publicly available. I agree that all of it should be available to the oversight groups, but I'm trying to gauge -- I think there is a -- As much as there are real and credible issues, there are also significant perception issues. And part of the way you address some of the perception issues is by providing more information rather than less. But I think it's useful for all of us to try to think of how to provide the more without actually impeding what the program is designed to do, yet creating greater assurances in the public. So, I think, you know, that's something that perhaps both of the Committees need to wrestle with. I think it's something that perhaps the government could use some greater guidance on.

MR. ROSENZWEIG: Last question for Anna before we move on.

MS. LEMMEY: I thank you for coming. I think your recommendations are interesting and very on-point in terms of defining the scope which seems to be the point of the biggest issues. Your comments about retaining data, you described them keeping the data until 72 hours post-itinerary completion. That triggers for me the question that in the PNR that was discussed, are they keeping full copies of the itinerary in order to know when that completion is over? Do they know the completion date? Which, obviously, for some of us who travel a lot changes frequently. And I know from the law enforcement work I have been involved in, the intel community, that the actual travel patterns are a critical part of the intel, if you want to look at flow of information and people. Did that come up and did you talk about the usage of that may be at some point in the future, if not now, and how you guys would perceive that usage?

MS. SLOMOVIC: We had very little discussion on the use of Secure Flight as an intelligence tool, and that was actually one of the reasons we said this could be a goal of this program. If it is, it should be exclusively stated as being a goal of this program, and then what data is collected and how long it's retained becomes a question relevant to that use, as opposed to simply doing the matching, which is a very different use. Doing the matching is kind of a static thing. Trying to track travel patterns is a dynamic thing. So you would need different types of data and different types of analysis. In terms of keeping itineraries, it's really up to what is in the PNR.

You know, sometimes people buy one-way tickets. Sometimes they buy tickets and change them. Sometimes they might also -- You know, it really differs from person to person, itinerary to itinerary, and system to system. And that's why we were very skeptical about the fact that PNRs would only be pulled before the initial flight because, of course, things changed. So if they have to pull PNR before every scheduled flight on the itinerary, then we question why it would need to be retained for the entire duration of the itinerary.

One possible reason given was that if something happened after the flight lands -- while the flight was in the air, then they would need information on that flight to determine what went wrong. But that's something -- that information should be retained until the flight successfully lands, not hours or days afterwards. So the whole retention question is kind of -- was not addressed very well.

MS. LEMMEY: But under the PNR you looked at, the information would be there to do the dynamic analysis at some point, at least for the current set of flights, and that may be one of the reasons to limit it to name and date of birth.

MS. SLOMOVIC: For the current set of flights under the current arrangement, yes. Theoretically, the data would be deleted within 72 hours of itinerary completion, so past that, you wouldn't have the data. Plus, if you have different types of itineraries, for some people, you would still have the data from their flights months ago, and some people you wouldn't. So the question is whether the quality of the data is going to be useful for whatever you want to do anyway.

MR. ROSENZWEIG: Thank you very much, Anna. The others have said so, but I want also to express our appreciation for your last minute -- both your willingness to come at the last minute and give a summary of your report and rearrange your own schedules to be here with us. We very much appreciate the work that your group did, and as Howard has said, if we seek proper, it will be because we have stood on your group's shoulders. So thank you for coming.

MS. SLOMOVIC: Thank you for having me.

MR. ROSENZWEIG: In a celebration of democracy, we're now going to hear from the program director about whom the report was written.

MS. SOTTO: We had the pleasure of hearing from Justin Oberman inform the Committee. Thank you for joining us again today. We're very interested in your response. Very quickly, for those of you who have not heard Mr. Oberman speak before, Mr. Oberman is the assistant administrator of the Office of Transportation of Vetting and Credentialing, and he is responsible for the development, testing, and implementation of the Secure Flight program. Thank you, Mr. Oberman.

MR. ROSENZWEIG: And if you would, Justin, keep your comments to about five to seven minutes because I know that the members all have questions.

MR. OBERMAN: Yes, and I now know the rule about how the flags are stood up and so forth, so I won't make that mistake again. Good morning. It's great to be here. Obviously this is a critical component of what we're doing, and I'm very glad to be here and have spent time with you in Boston and, of course, a couple other sessions in Washington. I look forward to continue to do that between now and the end of the year as you move towards some of your key outputs. Let me just address three substantive topics and then give you a minute or two on the status of the program. Those topics are scope, data, and contradictions.

Let's talk about scope. The objective of the Secure Flight program is to identify known or suspected terrorists threats before they board commercial flights in the United States. Period. It has been that since we rolled out Secure Flight 13 or 14 months ago, and it remains that today. So there are a lot of activities underway associated with that mission. There are a lot of areas of inquiry that are very useful, particularly for an entity of the size and scope of the U.S. government to undertake for a program of this size and scope. There are other views on that topic, probably as many views as there are people who are aware of Secure Flight, but that is the objective, that is the scope, and it hasn't changed. So I wanted to just make that very clear.

Now, with respect to this issue of data, it's a great point. It has been my number one concern since the day I took this job, and it remains my number one concern today, which would lead some people to think I've had a great year. I don't know that I'd necessarily put it that way. But that number one concern is still number one. And here's the issue. The single greatest challenge that we have with respect to standing up the program is acquiring the needed information from the air carriers. And the reason for that, and we've talked about this before, is because the airlines are in the business of managing their own reservations for their own sales and marketing, operational purposes, and they are -- many of them are using systems that are decades old and that are not designed to be extracted from and have data sent to another source; in this case, the government.

So we have been in dialog with the airlines for at least the 13 months that I have been in charge in a very detailed way on this exact topic, and we have tried to structure this program in a way that is as flexible as possible for the air carriers, while enabling us to achieve the mission that I articulated earlier. So, for example, if a carrier wants to send us an entire PNR, they can do that and we will filter it. There is no question on whether we have filtering technology. That's probably the single most important functionality of the technology that we have, because even if I only get the name and date of birth from an air carrier, I have to filter it differently than what I get from another air carrier. It's not going to be the same. So the filtering technology is the single most important thing and what we've spent a lot of time and effort to develop. If carriers want to send us only the name and date of birth, that's okay too.

Now, of course, just the name and date of birth, in and of itself, is not sufficient. It's sufficient for us to determine whether that person is on the terrorist watch list, but it's not sufficient for us to operate a passenger prescreening program for domestic aviation. We have to know what airline the person is flying on, we have to know what time their flight leaves, and there are various other pieces of data. When our regulation is issued, it's going to delineate those all in public. It's not a secret list. The only biographical data is the name and date of birth. So I want to make that very clear. While I tell you that, this varies among air carriers, as everything in aviation does, about their ability and desire to send us the bare minimum that we've requested or a greater list of information. And so I want to make that very clear. And the carriers have said, across the board, "We want to send you everything." "We want to send you only portions of it." "We want to use XML messaging format." "We want to use EdiFacts format," which is a global standard. "We want to use other approved formats that you say are okay." And we have said yes to everything. So I want to make that point very clear. It's a critical point, and it's very important.

The subtopic to that is, again, getting to this issue of effectively matching against the watch list and effectively mitigating both false-positives and false-negatives. So there is other information in the PNR that shows up very, very rarely. So I want to be very clear about that. But that can be extremely helpful to us. And in this game of matching against the watch list, extremely helpful has to do with how accurate you are. It doesn't have to do with how frequently you're able to do something. I want to make that point very clear.

So, for example, we have had on numerous occasions the usefulness of a phone number or an address, not for domestic aviation, Secure Flight -- obviously, it's not launched -- but the dozens of other vetting programs that I oversee where a phone number and address have been extremely useful at establishing that someone is, in fact, not on the list, so mitigating a false-positive, or, in turn, determining that someone is, in fact, on the list, even though their name and date of birth that we are using to vet is incomplete. That's mitigating a false-negative, making sure we don't miss someone who is, in fact, on the list. So that information would be of use to us.

As we all know, there are many people on the watch list who are not U.S. citizens or even legal permanent residents of the United States. They are foreign nationals. And there are a comparatively small percentage of people flying every day in the United States who are foreign nationals or legal permanent residents. And so having a passport number and country of issuance has also, in our other vetting programs, proven to be extremely helpful. So we're trying to work through all that with carriers, but the regulation is going to very clearly delineate what's required, and the carriers are going to be working with us point-to-point, each of the 63 separately, on a very detailed data transmission program that will describe how this data comes to us. I just want to be very clear about that. And our ability to filter is necessary whether they give us an index card with someone's name and date of birth or a 66-field PNR that came in on ASCII text form from 1968. We have to be able to filter that and vet it through our system.

The third topic I wanted to address very briefly is this issue of contradictions. And I think Secure Flight is a top candidate across all federal programs for having contradictory points of view, not only in different camps but among the same people. So this issue of how long to keep the data, it's a great issue. It's a great issue. It's been top-shelf issue since the day I took over and before. But there's a contradiction there, and I just want to make sure we all recognize it as a contradiction and recognize that there's also no easy answer. So you've got to look at this in the right context. Taking information into the government, comparing it against the terrorist watch list, and discarding it 30 seconds after that comparison is done, in my estimation, is not one-quarter as effective as keeping it for 120 seconds after it's done. That's not the way the concepts should work.

So we've got this issue of making sure that somebody who has booked a round-trip ticket and wants to have both boarding passes before they leave -- issued at the home airport, for example -- and making sure that that person doesn't present a threat. We have a very dynamic system which people change their flights all the time, obviously. We also have a very dynamic system in which the watch list is being updated continuously. So we have to be able to manage through all that. All of the regulatory documents, of course, are going to be subject to public comments and so forth, but I want to make sure we're talking about this on the right level, which is: Let's think through, if we start at that objective of the program, which hasn't changed, how we get there. I think getting drawn into that extended debate is okay, but it's not speaking to the fundamental issue as to whether or not we're structuring the program overall the right way, and it's not speaking to the fundamental issue of whether or not we're setting up a program that we're spending a lot of time and money on and making a big change in how people travel. That's actually effected in doing what our mission calls for. And so, I just want to illuminate that. I don't have any easy answer. If there was an easy answer, it would have been done already. But I just want to point out that inherent to all this are numerous contradictions on top of one another, and we have to be able to sort through that.

So I can provide more information on sort of where we are today, the latest and greatest September 28th update, or we can open it up for questions.

MR. ROSENZWEIG: When last we spoke to you, the rollout for live testing was sometime in September. We're at September 28th. Could you just tell us when you anticipate live testing, as of today, okay, knowing that all government programs get delayed?

MR. OBERMAN: That's a very good place to start. Let me say a couple of things. We have made numerous changes in how we administer the program, given the concerns that GAO raised about various aspects of our testing and that I addressed in my testimony in June and so forth. And so we made the determination that we had to amend our privacy documents that we used for testing before testing last fall, before we could start so-called live testing. And so we're in the process of amending those documents.

We're working with Nuala's office to do that. And those documents need to be amended. I think it would, in the quiet, you know, confines of the conference room, you can have a reasonable argument about whether those documents really do need to be amended. There's some very close calls in the Privacy Act. But we're not in the business of making close calls in the Privacy Act, so we're going to amend those documents and make those changes.

What I will tell you, though, is that we are on track with our system development to do live testing and are able to run through made-up records, and that is going to start, in fact, I think, tomorrow. We didn't drive "September 30th at midnight," in a typical TSA sprint, but we are going to make that September date. And, again, it's able to test the system end to end, but we're using bogus records, so to speak, because we have to make changes to our documents.

MR. ROSENZWEIG: That's great. We will have questions. And just to remind the members, typically I'm going to refer to people who haven't asked yet and give them a shot. Michael.

MR. TURNER: I want to begin by thanking you for coming here, actually, to consecutive meetings, given developments. I'm curious. Since we met in Cambridge, results were released concerning a pilot that you undertook. Could you just discuss briefly the findings, the top-line findings from that pilot and the length of the pilot, whether or not in your assessment the pilot was efficient in terms of its ability to find statistically significant outcomes and whether or not you characterize those findings as encouraging, particularly in light of potential alternatives for use of commercial data in Secure Flight?

MR. OBERMAN: That's a great question. A couple things. I would say that the results were statistically interesting. I don't think we were able to do a thorough enough inquiry to judge them to be statistically encouraging. I think that things are -- some of our hypotheses were sort of starting to form out in terms of usefulness of commercial data to verify identifies and mitigate false-positives and so forth. But it was about a 90-day test and, therefore, not adequate to sort of undergird policy decisions of this magnitude. You know, our only focus now is to stand up the aspect of the program associated with matching the names of people who fly with the names on the watch list, so we've ceased our commercial data testing so that we can focus exclusively on that.

I am interested in talking about alternatives in the context of the paper that the Committee has done, which I reviewed. I think it's an excellent piece of work. But I have additional discussion topics I think would be worth us pursuing, and I would put them under the heading of "alternatives," with probably a capital A.

MR. TURNER: If I could follow on that. Was there any significant learning from the pilot program that would have led you to have made statements that might imply alternative uses or mission creep in terms of objectives for Secure Flight?

MR. OBERMAN: I don't think so. I mean, I guess it depends on how well Google is running that day, whether you're able to find other things that are said on this topic. But I don't think so. In other words, the purpose of the program is to identify known or suspected terrorists before they board commercial flights in the United States. That's it. That was always what the commercial data test pointed to with this additional piece of trying to mitigate false-positives, which is a resource issue for us and a convenience issue for the traveling public. But, no, there hasn't been anything beyond that. We very narrowly tailor everything that we didn't test to those objectives.

MR. ROSENZWEIG: Jim Harper, you're next.

MR. HARPER: I'll just say that there's persistent confusion about scope up here, so we might need to have some more clarification. But I am interested in the commercial data questions. And I specifically want to understand better this business from a commercial provider's perspective, and I wonder if you could provide us the contract that TSA had with legal force so we can understand the business model, frankly: how they get paid, what do they get paid for, so on and so forth. I'd like to just be able to read that document and get a better handle on how that words. Can you provide that to us?

MR. OBERMAN: I think we can. I want to check with counsel because that's the kind of question our lawyers want to weigh in on. I can't think of a reason why we wouldn't be able to release it. I'd just have to check. But I guess I just need to say, to follow-up on that, under this issue of alternatives, this business model to me isn't, like, a fundamental issue, so -- It's worth further discussion. I wouldn't view that arrangement as dispositive or the way it should be and so forth. You know, it's a test.

MR. L. HOFFMAN: Thank you. And thank you for joining us again. I know you had some interesting comments for us in Cambridge. About what you just said, I am concerned that -- You just mentioned, in answer to Jim Harper's question, you're going to check with your lawyer again and get back to us. My concern is that coding and testing goes forward even as the system specification, the providing information, and, you know, you try to get there, but "We're going to code away anyway." It almost seems like it might be --

MR. OBERMAN: We've ceased all activity on commercial data testing. There's no coding --

MR. L. HOFFMAN: I mean, in general, in the program. I'm not speaking only on commercial data testing. I'm speaking in general. I'm concerned that the -- For example, we got in our briefing packet on the U.S. business program -- I have this much information (indicating), a whole stack of documents, and charts, and schematics and so forth on US-VISIT. I think they have had no more time than you've had to develop a program -- correct me if I'm wrong -- and yet that's something at least I can understand. I sort of get a sense of where things are going, where they flow from and to. I haven't seen that -- maybe other groups have seen it, but I sure haven't -- and that concerns me, that the system specification and documentation seems to be not available. And just as importantly, not only about Secure Flight -- I understand you have management of a dozen or so other programs -- the interoperability and how things operate or don't, what the controls are between and among those programs doesn't seem to be specified in a coherent manner; not in just English, but in real life schematics. Maybe I've just missed something, but I'd like to find out if you can comment on that, and also if you could provide us with those things and, if so, when.

MR. OBERMAN: The answer is: That does exist, we can provide it to you, and don't mistake me when I say I'm going to check with counsel. It's sort of like, "What time is it," and I'm, like, "I'm going to check with counsel." That's the way I have to do my job. And so we'll get it to you. I have more than you would be able to consume in terms of schematics; of the other programs, Secure Flight, system designs, what the coders are coding. So we can provide that to you.

MR. L. HOFFMAN: Why didn't the other group get that, Anna's group, or --

MR. OBERMAN: Yeah, I think -- A couple of things. I'm not satisfied with the way that process worked overall. So, as we discussed before, we're going to make sure as a matter of policy that whatever was requested that wasn't provided will be provided to this group, since that group is disbanded, and this is providing an oversight function. I think the second thing is that there were some timing issues with respect to the fact that many documents did not exist at the time they were requested, and I will just say for the record that US-VISIT has been in existence a lot longer than Secure Flight, so they've had a lot more time to put a lot of this stuff together. And, you know, we will get you the details. There is so much technical information, it's incredible, and virtually all of it has already been turned over to GAO. So...

MR. LANCE HOFFMAN: The final question I asked was when -- Approximately when will it be turned in?

MR. OBERMAN: Yeah. I think the answer is: very, very soon, because all the documentation exists. I've just -- I've got to run it through traps at headquarters, and then we'll get --

MR. ROSENZWEIG: For the other Committee members at the screening subcommittee, after three months of speaking with Secure Flight and TSC, we have, essentially, a list of dozens of things that we want, and we're going to have that through our subcommittee in a letter of request. I assume the letter will get out from us promptly. Right, Howard?

MR. BEALES: (Nods head.)

MR. ROSENZWEIG: And it will be equally prompt in getting us back answers. So if you have the takeaway, for the Committee members, if there's something you want to be on the Secure Flight list of document requests, please transmit it to Howard, and it will get on the list. And the request list will be made public. The responses, obviously, may be subject to classification issues, but the request list will be public.

MR. BEALES: Paul, I just wanted to interject. In all of our dealings and requests for information, TSA has been quite forthcoming and quite willing to provide us with information. We have not had the experience that the Secure Flight Working Group obviously had of feeling frustrated by the ability to get information, and I have every hope and expectation that that will continue.

MR. ROSENZWEIG: We just raised the bar, Justin.

MR. LEO: Thank you for being here, as well. Please forgive me; I'm a nonlawyer, so --

MR. OBERMAN: So am I.

MR. LEO: -- my questions will be very pragmatic. One is that I'm going to lead to the issue of consequences. So to get there, first, there appears to be an agreement that there's a fundamental right to privacy of U.S. citizens, fundamental to the basic law of the formation of the country. Secure Flight seems that it overwhelmingly does something to check on U.S. citizens, that the population that you're going to get is huge with regard to U.S. citizens. So therein lies the second thought, which I have, which is the access to information about folks is a privacy matter, so there's got to be some sort of metric that says, "Well, if I have a fundamental right to privacy, what's the metric that's demonstrating that I have that privacy?" In other words, "If I have it and the metric shows that, no, I don't have it, then there's a disconnect," which leads to the question of consequences, which I'd like to ask, which is: Well, then, what are the consequences, assuming the government does -- and everybody seems to agree, as far as I can tell -- the government will take this function, that TSA will do the matching program? So when the government inherently takes over the function, it then has responsibility, and responsibility has consequence, if it doesn't do what it says it's going to do? And I think that's why there's a lot of apprehension and a lot of questions. So I would like for you to dwell a little bit on consequences of the Secure Flight and behavior of the government to ensure that there is the fundamental right of privacy and how that is protected, which I think is part of our reason for existence of this kind of question.

MR. OBERMAN: That's an excellent question, and I'm not that sure there's a clear, crisp answer because privacy is about as personal a sentiment there is. I don't know that there's a metric. You know, number of data elements submitted to U.S. government for domestic flights, seven is too many or something. I don't know what it is.

What I would say is a couple of things. We have four key privacy principles for Secure Flight that we have had in place from the outset. And, you know, I think that adherence to those is critical, and I'll get into those in a second. I think that oversight of the program is essential from Congress, which we certainly have; GAO, which we certainly have; and Committees like this, which we certainly have. I think that's critically important. But the issue of consequences is fundamental. I mean, it needs to be thoroughly explored, you know, forever, even after this program stands up, because, you're right, everybody will agree, keeping known or suspected terrorist threats off of commercial flights of the United States is a worthwhile goal. But if it starts to spread from that, you are going to have the potential for much greater consequences.

So the importance of the privacy principles, I guess the only thing I would address is, you know, this is one of the challenges we are faced with after 9/11, which is commercial jets were hijacked and used to commit attacks on U.S. soil. So every system that's been put in place since then to protect against that and the next generation of threats automatically impacts a huge number of U.S. citizens, more so than what happens on the border, for example. And we were hit at home, and it's affected all of us and will continue to affect all of us moving forward. I don't have an answer for that. You know, people are moving freely around the country. Now, with respect to the privacy principles which we put in place and we tried to adhere to for the purposes of mitigating some of your very well-articulated concerns, they include the following.

Number one, we are looking to identify only known or suspected terrorist threats. This program is not looking for people with criminal violations or deadbeat dads or people who are Vikings fans or anything like that. We are focused on known or suspected terrorist threats. That's number one.

Number two is, we have and will continue to articulate the fact that we're collecting only the information we need to effectively perform our function. Now, when you're talking to 63 air carriers, many of whom are suffering financially, many of whom have very antiquated systems, you can adhere to the principle that you only use what you need. But it gets a little bit tricky to appear to the principle that you only receive what you need. And that's what I mentioned before. The carriers of are a very heavy lift with respect to technology, in terms of sending us only what we've asked for. So filtering data is the first gate in our system. You'll see that in all the schematics. And the information that's not used for vetting is immediately discarded and never reviewed by anybody at TSA. And the schematics will bear that out.

The third piece is keeping the information for only the time that we need to perform our function. So we're not keeping it for 50 years. We are going to keep it while somebody's moving through the aviation system, for obvious reasons, but as soon as they stop moving through the aviation system, that information gets discarded.

And then the fourth principle is that we are subject to numerous statutes and regulatory requirements with respect to disclosing what we're doing and having restrictions on how this program can expand in scope. So tomorrow if I wanted to use this program to look for something other than potential terrorist threats, there are a series of hoops that we have to jump through. But with good reason. That keeps us safe. It's hard for us to issue regulations because that's a limit on the government which is desirable, particularly in a field of this type. So that's why we have to issue regulations, system of records notices, privacy impact assessments, Paperwork Reduction Act notices, separate IFRs we want to exert, exemptions to the Privacy Act, and the list goes on and on. And that's a complicated process that's complicated on purpose, at least a complicated process in my view, and it helps mitigate some of these potential consequences that you get.

But on the issue of consequences, that issue will never and should never go away, in my view. It just --

MR. LEO: Can I just ask, under four, or five, that when you come out, etcetera, that the public will see that, "consequences"?

MR. OBERMAN: Yeah. I think -- Here's my view on that topic. It is presumptuous for us to try to articulate sort of, "Here are the consequences for you," because that's not giving the public a chance to try to identify what they think the consequences are. So, for example, we are going to say very clearly that we need people's names and dates of birth to identify known or suspected terrorists before they board commercial flights, but we're not in the position to know what 280 million people think the consequences are in their right to privacy. So, I don't disagree, but I don't want you to think that I can just state what the consequences are and then those are the consequences. That's sort of contrary to how this disclosure process is supposed to work, at least in my opinion.

MR. ROSENZWEIG: As we move on, I'll alert the Committee members: We're going to change the schedule on the fly. I see nods because I've heard from already several -- We're going to continue to 10:30 with Justin, take a break. We're going to just skip the subcommittee reports, hopefully get to them in the afternoon, dispense with them. We're going to eat -- at least 15 minutes into the next panel, and then take time out from lunch so the next panel will get its full time. But with respect to our guests, we'll start about 15 minutes late on that. I will also remind the Committee members, I note that you all have lots of questions that Mr. Oberman will be joining us for a briefing on Secure Flight, including some of the classified aspects, at the close of lunch. So if you don't get to your question now, you'll have another shot. So don't feel too bad. And if you have questions that you want answered here in the public forum, better to preferentially choose those. Next on my list is Reed and then Charles, and then I think that will -- And then Joanne and David will have, I think, eliminated the ones who have asked before.

MR. FREEMAN: Thank you, Mr. Chairman, and again thank you, Mr. Oberman, for coming all the way out here. A couple of very focused questions. You mentioned that you're working on revising the privacy statements and a regulation is forthcoming. What level of specificity can you give on the "when" part of that?

MR. OBERMAN: I think your mic's broken. It's very difficult for us to say when. I mean, I hope that it's measured in weeks. I think it is, but it's very difficult. You know, these documents are sent to review by numerous parties. I think more people ended up reviewing the documents outside my organization than are actually in my organization working to stand up Secure Flight. But on something of this magnitude and importance, screening two million people a day, I think that's warranted. So it can get frustrating for us because we're all anxious to get going, but I think we will have a better process for it after the process is completed. So my hope is that it's soon, but it's not tomorrow. And as I mentioned, there will be a regulation in about five or six documents associated with it. So it's a very hefty package to move through the coordination.

MR. FREEMAN: A separate question: What form of report or set of recommendations from us would be most useful to you in your job to fit into the development of your program? Can you give us any guidance on how we can best plug into your process?

MR. OBERMAN: It's a great question. I think -- Well, personally, to the extent that you have recommendations associated with certain privacy policy issues, this issue of consequence, and so forth, those ought to be public recommendations, and I would expect that we will concur and then be able to respond publicly. So I think that's important. I think if you have recommendations based on your review of some of the technical information about technical changes, I think we'll have to look at that case by case as to whether some of that should be public or not. You know, we can't compromise the system. But the more important part on the technical recommendations is, the sooner the better, because we have a major development effort underway; you know, dozens of people every day coming in and trying to put the finishing touches on, and if there are things that you think need to be adjusted, we may have to do that verbally or something so we can do it. But with respect to privacy policy data handling, it ought to be public. And then we'll come back and follow up. I think that's what the Secretary wants.

MR. ROSENZWEIG: Charles, you get the last one before the break.

MR. PALMER: Thank you. So since the topic of our Committee includes data and integrity, you had mentioned these 63 carriers and their variously antiquated more modern systems. Can you say anything about the security, integrity, and flow of the information you get from them? Blasting little ASCII files didn't sound particularly robust to me, but I was wondering what you think about that and how well the data flows are and how they are protected? Because I like to break things, thinking this might be an easy one.

MR. OBERMAN: Well, a couple things. Firstly, I think -- You know, a couple things to keep in mind. We have a major effort underway, which is actually nearing completion, because we're able to sort of manage it internally and get it done, unlike most of the rest of this program, and it has to do with having overall certification of the system's security. And there's a separate team of folks who work for me that are doing this. There is a list of documents, literally about 18-inches high, that describe all of the security architecture that's in place, and that's accompanied with a repeating series of tests by outside parties to try to break the system. And, you know, that system doesn't get certified as secure until all of those requirements have been met and the Departmental CIO independently certifies the system is secure. And so we can walk you through that in more detail, if you want, but there's a very heavy requirement.

A couple other things I'll mention. Very unique to Secure Flight, we're trying to win the title of unique program attributes at DHS. We're, I think, in the lead. GAO is actually going to re-review all of that security certification, which is unique because it's a statute that requires us to do the security certification, but now Congress has said in addition to that statute we have another statute that says GAO has to review it. So, that whole stack of documents, all the testing that's been done and so forth, will be re-reviewed by GAO.

And then the third thing I would say is, I would welcome the chance for you to come and spend time with our staff. Transmission issues are extremely important in addition to what happens once it is received by TSA. I will tell you we are working very closely with Customs on this issue because Customs already has connectivity to the major U.S. carriers for international vetting. We're going to leverage that connectivity, as they have had many years to perfect the system and make it secure. But I will never turn down help on an issue like systems security. So... We have done an incredible amount of work to make sure the system is secure, but I would welcome further help. It'd be great.

MR. PALMER: And just a clarification, the concern is not only your own systems but getting this information from the carriers.

MR. OBERMAN: Yeah, absolutely. I guess I would tell you -- You know, we could spend time with the airlines. It would be worthwhile to have them describe systems security. They have an issue not only from a security perspective but also commercial perspective because they've got reservations, data, they have to bill people, and so forth. So we can -- That's an open door. I can hook you up with carriers to talk to them about it and have you talk to our staff, as well as Customs, about the security transmission. It's a very worthwhile topic. I think it would be helpful to us. That's easily done.

MR. ROSENZWEIG: On that note, we will take a 15-minute break. (Recess.)

MR. ROSENZWEIG: I've got four more people, and I will cut it off at that in light of the classified briefing afterwards. So, I have Joanne, Kirk.

MR. ROSENZWEIG: I've got three more people. Okay, and Howard. We'll give Howard the last word as chairman of the Review subcommittee. Joanne.

MS. McNABB: One of the privacy concerns that many of us have with any kind of screening program is the problem of people who are wrongly identified and inconvenienced, or worse, and I wanted to know what kind of redress procedures you have considered, whether you have any documentation of what various opportunities might be and where you're going on that issue.

MR. OBERMAN: I appreciate you raising that issue. And let me just say a few things about the topic of redress. First, let me -- Just for clarification purposes, and I will do everything I can to make sure your request is -- There won't be an issue there. But the Redress Office is independent from our organization on purpose because we want a dedicated team whose only mission is to provide relief for people if, in fact, they have been misidentified. So, Paul, however you want to do that. Logistically, we'll work with -- I'll just make sure you get connected with the Redress Office directly in terms of documents and so forth. There are significant bodies of documents that have been developed and so forth, and so I think we can get that to you. I've just got to -- Well, I'll facilitate. A couple of things I want to mention.

We have a redress process in place today at TSA that actually works quite well. We receive thousands of requests a month from people who have been misidentified at the airport as potential watch list matches, and they are provided relief usually within a matter of days. It often takes longer. That is not well-known. And I think it's not well-known for a couple of reasons.

Firstly, it doesn't have "Secure Flight" in front of it. The second reason is because once someone is provided with redress, which means they're put on the list of people who are, in fact, cleared and do not present a threat, that cleared list is administered by 63 separate air carriers in slightly different ways, which leads to people who are on the cleared list who have completed the redress process continuing to get flagged at the airport. So when they continue to get flagged at the airport and they've run for president in 1980, like John Anderson did, or they're existing members of Congress and on and on, then the news is: Well, redress isn't working at TSA. So what I will tell you is two things. Number one, we'll have consistent application of the cleared list under Secure Flight. The system doesn't care whether you're on American or Delta. That's why the filtering function at the beginning is so critical, because I have to make all the data standard, even if you've only sent in the name and date of birth. So that's number one.

The second thing is, we're taking a process that works and we're upgrading, so there will be a bigger staff of people, they will have new technology tools, they will be directly tied in with Secure Flight in an automated way, and have access to our passenger information if they need it to perform redress. I mean, that's part of the whole point, because what happens today is that they have to reach back to the air carrier and get the underlying travel information, which is very cumbersome and very poor, very slow. So that's one of the reasons we have this 72-hour retention period, so in case we have to perform redress, we can access the records and so on and so forth. So that operation is going to be significantly upgraded. It will have more standing in the organization and so forth. But I think we are building on a system that is bigger.

Now, I don't want to answer there and dodge the critical issue, so I'll just mention it and let you know we're very well aware of it. I think that what many privacy advocates are referring to when they complain about the redress process is not our ability to put people on a cleared list; in effect, that one airline might run it differently than another. Those are legitimate, and it's a big hassle, big strain on resources. But the problem is about as big as it appears because you have very well-known people who have gotten flagged. What they're getting at is this underlying issue of whether someone actually presents a threat if, in fact, they're on the list. And what I will tell you is, you're going to have to get some of these details from the Redress Office because I've got an arm's length relationship here, but they are going to have their own relationship with TSA screening center and other agencies to work that issue if, in fact, it turns out someone does not, in fact, present a threat. And so they'll walk you through all that.

I think that the Executive Branch overall has done an excellent job of continuously reviewing subjects on the list to ensure that they do present a threat. I will tell you from my own experience in talking to case agents that work these cases, if they feel that someone has been inappropriately watch-listed or was watch-listed appropriately but no longer presents a threat, they are the first to say it. I have had that experience universally. So that's a big deal with respect to redress. I think our business processes with TSA are going to be excellent and provide very excellent service to people.

MS. McNABB: Can we have someone come to us at another time from that office and --

MR. ROSENZWEIG: I already wrote down "contact redress office."

MS. McNABB: Thank you.

MR. OBERMAN: Let me just say one other thing on that quick topic. The redress folks have been heavily engaged with GAO, for example. So -- Becky's nodding her head. I agree; I think they will be happy to talk to you about that. Becky, and I agree. That's easy.

MS. LEMMEY: First I would like to say we thank you for coming again. I think we all respect the fact that you are in an enormously difficult position, because there's not really a good answer to a bunch of this stuff. And I know you constantly feel like we're attacking you, but we're not; we're trying to figure it out. They're a bunch of issues I want to raise, and they're a little bit higher level than where we've been so far.

The first is the scope issue. You described the scope in your beginning -- you talk kind of fast, so I wrote it as quickly as I could -- "identify known or suspected terrorist before they board a flight in the U.S." "Commercial" might have been in there; I'm not sure. To me, that's an enormously broad scope, and it's also the mission of the FBI. And I think that there's an interesting issue about the crossover of whose job it is to identify known or suspected terrorists and get them before they do anything, including boarding an aircraft. So, to me, that scope issue is big. That's not a limited scope. And it sort of concerns me that that role is off as a limited scope, when it's very, very broad.

And that brings me to my second point, which is, I think that a lot of what's making folks concerned is: Whose job is this, really? Is it the FBI's job? NCTC's job? And people who have struggled with the issue that rights come from wrongs or clarification of rights come from wrongs, they've already been through a lot of what you guys are struggling with now, because they have a lot of barriers to take this kind of information into the government in any way possible, not just identifying people but also -- I think a lot of U.S. citizens would be very concerned with their itineraries going to the government, not just their names. I think it's interesting that everybody keeps coming back to saying that this needs to be centralized, because when we look at the goal in the long term -- not your goal, not the goal of your organization but the goal of national security in intercepting or identifying known or suspected terrorists, we're going to have to move to a decentralized system in order to look at where that intercept might happen. And so the fact that this is an initial pilot that's moving to a central place -- and we can talk about the industry issues of the airlines, although I don't think they are necessarily completely relevant here. I think that we're being drawn into using this project as something that's actually a much bigger issue in front of discussions. And so that really informs and concerns me.

I also get concerned when -- as Joanne points out and others before have pointed out, there's not a lot of transparency in many people's relationships with TSA where they have intercepted them. You know, I was accused of having bomb stuff -- you know, explosive materials on me and got put on a paper list at the airport and had no way to get off of that list. Having just come from a White House meeting, before going there, I'm pretty sure I didn't have bomb stuff on me. But I think it's those kinds of things that cause consternation. The bigger issue for me is looking at this -- I recognize we're fighting a lost war in some ways, that there's a hyper set of intentions to this particular set of issues because we don't have an MI5-like object here to deal with what these crossovers are, pressures ending up here, when it might really belong somewhere else. What are your thoughts about that? And, you know, I recognize you're put in this position because of where congress put it at the time, but, you know, do you think that that should be rethought?

MR. OBERMAN: So, Paul and Lisa, I don't want to play any favorites, but this is my favorite question of all time. And I'm very glad you asked it. I have a few close friends left, not many, and this is what was talked about at midnight on the way home from the office. And it's an absolutely crucial issue of what we're really doing. So let me say a couple of things.

Firstly, I agree that there are multiple ways to interpret keeping known or suspected terrorist threats off of commercial flights in the United States. But other than commercial, there are statutory requirements dealing with chartered flights and so forth. The way that's structured in the entire format is that they kick in after we've stood up Secure Flight for commercial traffic. But you should be aware that that's in there. So let me say a couple things. What we're going to stand up is comparing the names of people who fly on commercial flights domestically with the names on the consolidated watch list from the terrorist screening center. So, writ large, it is the, quote, FBI's job to identify known or suspected terrorist threats. As you know, the overwhelming majority of those records from Terrorist Screening Center are from the Bureau, but, of course, there are other agencies working the issue. The way this is going to work is, when we identify someone who is on the list trying to board a flight, we are going to notify the FBI; we're going to notify -- First we're going to notify the carrier and say, "Do not issue the boarding pass and let the person proceed onto the airplane." We're going to notify the FBI. We're going to notify TSA at the airport so that they're aware and they're there to help. And then we're out of it. And that's the way that's been designed, and it's on purpose, because it is the FBI's job. Now, so let me just finish this thought. So what we're trying -- One of the major security benefits -- We've talked about privacy principles. I also have four major security benefits for Secure Flight, and one of those four is an organized, structured law enforcement response when you have someone who's a potential threat trying to board a flight. Today it's a very *ad hoc* system that varies greatly by city and by air carrier. So we're going to have a routine, structured way to respond which will be governed by the bureau who is investigating these people and is responsible for making sure that they are under surveillance and so forth. So that's number one.

Number two, we have an issue that is worthwhile to explore, but it's sort of worthwhile to explore on Track B because I am focused on Track A, which is: Names on flight, names on list, and are they a match. And that is this issue of trying to identify people that might otherwise present a known or suspected terrorist threat. What I will tell you is that I don't know that I would necessarily agree that that is solely the FBI's job in the sense that it isn't possible for the FBI to investigate -- and I wouldn't consider prescreening an investigation -- but it isn't possible for the FBI to review two million people flying every day. It is our job to protect the transportation of United States, with civil aviation rights at the top of the list. So that's a Track B discussion, not because it's less important. In some ways it's more important. It's just a track B discussion because our task right now is do names, names, compare, and off we go. And I think it is reflective of the fact that it is, as you put it, the FBI's job because we're using data from the FBI and we're handing off how to handle it to the FBI. And I think that's the right way to do it.

MS. LEMMEY: So just a quick follow-up on that. So you're acting in some ways as an agent of the FBI here or in that role. Now, what would their rules about appropriate use and collection? Because they've been through a long history of, you know, having been pushed back in a lot of places. And do you have different rules than they would, and are you applying that same set of rules based on your being an agent of them?

MR. OBERMAN: Yeah, I don't think that their rules on use and collection of, you know, data on citizens, for example, is necessarily where we want to start when we're talking about Secure Flight, because they're a law enforcement agency with the leading investigative authority for investigating terrorism in the United States. We are a civilian Homeland Security agency that has statutes and rules that we have to adhere to for collecting information; in other words, Privacy Act and other things that do not apply in the same way in the course of the investigation. So what I will tell you is that we have an excellent relation with the Bureau across these other dozen programs that I work on, and the rule is that when you find someone who is a match, you give it to the FBI, and you proceed according to their direction so that you don't tamper with an investigation that's ongoing. And that is, notionally, how it's supposed to work today and often how it works, but it's not routine and structured. And that's what we'll do with Secure Flight.

MS. LEMMEY: Just so --

MR. ROSENZWEIG: Tara, we're well past the time.

MS. LEMMEY: I just want to make a comment to the Committee, not a question, which is I think that the challenge we're seeing here is a challenge we're going to be seeing on a regular basis as DHS has to perform some of the duties that would be in intel or law enforcement and how would we address those questions to recognize that this is the first of many options here.

MR. ROSENZWEIG: Fair enough. This is the last one, and then we'll go on to the next panel.

MS. SOTTO: Thank you, MR. Chairman. First I just want to say that the goal that you are trying to accomplish certainly is laudable. We all travel a lot, so we thank you for trying to keep our air space safe. In the sort of "lessons learned" category, you've decided not to use commercial data to serve that goal. That issue certainly is not going to go away. We know that commercial data will be commercial data or potential -- the proposed use of commercial data will crop up time and again.

You said that there was a dual purpose for using the data. First was to reduce the number of false-positives and, second, to enhance -- I think I got this right, but if you'll correct me if I'm wrong -- to enhance the ability of the Department in its research on this area. So I'd ask you to elaborate on what that research is and how the commercial data might assist, and also to tell us the specific reasons as to why there was a change of heart in the use of commercial data.

MR. OBERMAN: Yeah, okay. So let me clarify the first point. We had two things we were testing. One was the ability to mitigate false-positives. The other was the ability to verify the identities of people who are flying. Under that overall -- Over those two objectives is this overall issue of having a body of work that would be useful, not only to us but to other parts of the Department.

So just to clarify that, those were the -- If you look at it that way, there's sort of a bullet and then two sub-bullets attendant to that. What I would say is -- Okay. So here's the issue on this, and I don't think it's a particularly big secret, but I'm happy to describe it. We had a limited scope test set up, and we administered it. It went very well. We ran it, as I said, for about 90 days, maybe a little bit longer. And we were testing various hypotheses, and we got some great results from it. You know, Michael's question was, is it statistically significant, and that's a high bar to determine on two million people a day. So I'm hesitant to sort definitively explain the table and this is statistically significant. What we did -- The reason I said it was promising is that some of our hypotheses were starting to be validated. Some were invalidated, which is also very useful. And it was sort of leading us to figure out whether and how this would be possible to do. What I will tell you is that it's a heavy lift for our team. I mean, there's a lot of work associated with trying to get this stood up. I do not have -- Contrary to what some people may think, I don't have unlimited budget and people and so forth. And, you know, we are just, you know, adamant and we know we have to do it ASAP to get the watch-list checking function done. And so as we were trying to figure out sort of how to drive that to a conclusion. We said, "Look, we've got to refocus. We're going to set this aside, and we're going to spend all of our time..." So, I don't -- You know, there really wasn't much more to it than that.

I think that GAO findings from the summertime and so forth were extremely useful to us. I gave an example already of how we've acted on that with respect to operational testing. But the truth is, there are certain things that we will always be able to disclose and can always be disclosing more. I think that experience proved that, and that's what we would continue to do in the future. So we're really focused on getting -- You know, we were talking about in the last question: Names, names, do the comparison. And we'll have to leave that work for another day. It's just a very complicated technique. I can't state it any more plainly.

MR. ROSENZWEIG: Thank you very much, Justin, for taking the time to be with us. As many have noted, this is your second appearance before us in three months, and we realize that we have trenched a great deal on your time. Added to that, the meetings we've had in Washington of the subcommittee. We all appreciate it as we work to develop an understanding of the program for the report that the Deputy Secretary has requested of us. We will look forward to a little more conversation with you in the classified lunch briefing, which should be in about an hour 40, an hour and 45 minutes. Go have a glass of water or something. And with that, our thanks. And I'll ask the next panel to come up and join us.

Maureen, do you have the name tags? As you're coming through, let me address all of the participants in the next panel. We have about an hour 45, and as you've probably figured out, the Committee members are very anxious to ask questions. If you have written statements that are in electronic form, we'll certainly take the whole thing and everybody will read them. I'd ask you to kind of keep your opening remarks in the five-to ten-minute range and -- I'll cough loudly, and then we'll have a great opportunity for more questions. Lisa.

MS. SOTTO: Thank you. In the interest of time, I'll introduce all of you together, and we thank you very much for being here with us. And you can choose whatever order you'd like. I will introduce you in order.

Michael Westray. Michael -- Mr. Westray is a senior member of the Information Technology System Integration Coordination Team at the US-VISIT Program Management Office. He's responsible for all technology initiatives and life cycle activities from the requirement phase to operations and maintenance and has particular experience with Radio Frequency ID technology.

Deirdre Mulligan is the Director of Samuelson Law Technology and Public Policy Clinic and an acting clinical professor of law at UC Berkeley School of Law. Previously Ms. Mulligan was staff counsel at the Center for Democracy and Technology in Washington, D.C. She is currently a member of the California Office of Privacy Protections Advisory Counsel -- Joanne, I'm sure you're delighted to have her here -- and a co-chair of Microsoft's Trustworthy Computing Academic Advisory Board. She's also on the advisory board of the Electronic Frontier Foundation.

Lee Tien is also with us. Mr. Tien is a senior staff attorney with the Electronic Frontier Foundation in San Francisco. He specializes in free speech law and privacy law issue and has also litigated Freedom of Information Act cases.

And finally on this panel, Peter Neumann. Mr. Neumann has been with the SRI Computer Science Laboratory since 1971 and holds two doctorates from Harvard and Darmstadt. Thank you very much. We'll begin with Mr. Westray.

MR. WESTRAY: Thank you. Nice to be here. I'll be very brief. I'm here from the US-VISIT Office. US-VISIT is an acronym for United States Visitor and Immigrant Status Indicator Technology. We realize that we needed to capture more entries and exits from our visitors in order to gauge the status of our visitors, in addition to targeting those that violate terms of their admission. Unfortunately, we were gathering, issuing people documents for travelers, but we were not annotating actual entries and subsequent exits. So we realize this is one of our charters. We spoke to Leverage Technology to assist us in our efforts. Business owners had created several high level requirements centered around low degradation of level service, low increase in inspection times, protecting privacy of all citizens. So we reached out, and we also performed an operational alternative analysis. We looked at global positioning, iris scan, retina scanning, hand geometry, passive and active RFID. And the anomaly with our system is that we must capture at exit. On vehicle lanes, sometimes that can be up to 50 miles per hour.

So this is, clearly, a long attempt for us. So, clearly, based on that, some of the technology is just not convincing. And we looked at passive RFID. Now, we did also perform a robust feasibility study. We built two lanes in Falls Church, Virginia. We performed over 600 tests. We had buses come through, personnel on buses holding tags up, and we were happy with the results of our feasibility study. We also looked at several form factors, embedded passports, embedded I-94s, and we realized that since we were getting over 90-percent read rates, that we would proceed on with the proof of concept. And this is what's actually going on in Blaine, at Peace Arch, Pacific Highway. It's also going on in Alexandria Bay, New York, as well as two locations in Nogales: Mariposa and Deconcini.

Now, that gave us a variety of weather conditions, a variety of traffic patterns, and operational conditions as well. Coordination and date. Before we even move forward, we talked to Johns Hopkins Applied Physics Lab, we reached out to the Department of Homeland Security Wireless Management Office, some industry leaders that were out there. We just wanted to get some input on the state of the technology even before we were to implement it. We're also a member of the DHS RFID counsel. And remembering IAC, Industry Advisory Counsel, their emerging technologies division, there are over 35 vendors that participate on the RFID Committee.

Right now for the proof of concept, the population is nonmember and Visa holders and those that also are traveling under the Visa Waiver program. Ages 14-79. This population has I-94s, if they're issued. Now, we -- They're very familiar with the process. They've been going through it in the past. The only thing that's happened now is we're issuing them embedded I-94s, which look exactly like the initial ones they were getting, and at issuance, we are linking the I-94 to the traveler biometric and biographic information which is taken at issuance. There is no personal information stored on the RFID tags, just a unique identifier. The population we're looking at is about 3.2 million.

And to date -- We started proof of concept August 4th, and we've issued over 50,000 I-94 tags, so I think we're getting a good gauge of the population and of the technology. We did perform a privacy impact assessment, and we also have a system of records notice. The system was also certified and accredited.

Again, the tags contain no personal information whatsoever, and they also are write-once/read-many tags, so, again, the informational tag cannot even be manipulated. Again, it is tied to the traveler at issuance, and all information which is gathered is then processed over secure firewalls of the partners' agencies and also virtual private networks. All hardware transmissions are regulated by the FCC.

Now, the evaluation. From September 9th through the 18th, we wanted to evaluate, again, the read rates we're getting here. Again, this is proof of concept. So, we're very happy. The Canadians were very helpful, and their officers are utilizing hand-held readers. So on that note, they would read these I-94 tags which came over to Canada, and that would serve as a denominator to show us that, "Hey, you should have read a thousand." We would then go back into our system and kind of do some number crunching and evaluation of our data to see what it is that we actually did receive. And lastly, I'll say that this initial proof of concept deals with issuance, pedestrian entry and exit. For pedestrian entry, there's a graphical user interface, so that when a traveler is approaching the officer's booth, information is displayed for the officer, which consists of a photo and, also, the watch list results. So, again, a lot of information is done before they even approach the booth. Now, that will give us a confirmed reading.

On pedestrian exit, subsequently vehicle entry and vehicle exit, the only thing we're doing for proof of concept is reading, and we're getting reported readings. Again, it's not confirmed. So hopefully I've shed a little light on Increment 2C, which is our RFID initiative, in ways that we're leveraging RFID.

MR. ROSENZWEIG: Just a quick clarification question. In the test where the Canadians provided the hand-held backup, what was the read rate? What was the success or failure rate?

MR. WESTRAY: We're actually in the process of crunching the data as I speak. The results of this proof of concept will be out on October 28th, so we're running the reports right now.

MR. ROSENZWEIG: Okay. Thanks. Ms. Mulligan, I guess you were next on the list, so we'll go that way. Professor Mulligan, I should say.

MS. MULLIGAN: I guess I want to step back a second before getting into the US-VISIT issues specifically. I think it's important to have a slightly broader perspective. So the US-VISIT and RFID are really part of this much broader conversation and a more complex conversation, but I have to just say we've pretty successfully avoided having, right, which is the about the desirability, function, cost, and benefit to the nationwide system of identification, and perhaps worldwide system of identification.

Right after September 11th, I was serving on a National Academy of Science Committee that was looking at authentication of privacy issues. And like all National Academy of Science Committees, we were asked to turn our expertise and our research towards thinking about what some of the questions that were likely to come out of our experience on September 11th that would be relevant, right? Well, how would our research be relevant?

And we issued a report that has the catchy but, I have to say, somewhat tacky name of "IDs: Not So Easy." Right? You'll remember that, thought it's a little tacky. I had nothing to do with that. And it raised many of the questions that you've heard earlier this morning about scope and purpose and the need to really think critically about what those are before you can engage in any kind of thoughtful examination of the system. And a purpose that as broad as keeping terrorists out of the country might not really provide us with enough to push up against. It's kind of like taffy. And so the debates about our ability to identify and authorize individuals have kind of permeated certainly our legislative history, and they've been around issues about entering the country, about the ability to work in the country, employer verification pilots, and most recently, whether or not it's appropriate to use the REAL ID, which was jammed into this appropriations bill, military spending bill, as a mechanism for determining who's can, you know, actually make use of a polling place.

And so I think, you know, when we face issues about whether or not we want to embrace nationwide or national -- both two different things -- whether or not we want to embrace that whole hog -- you can probably remember that through Larry Ellison's law firm, right, to supply us all with the technology to facilitate the creation of such a system -- it's been pretty routinely rejected both by policymakers kind of written large and also by DHS. And so -- but framed in the small, right, whether it's about the US-VISIT system or whether it's about employer verification pilot programs, which DHS now has some authority over too, the conversation seemed to fall away to the side about broader policy issues and we end up much more focused on the technical particularities about the read range of the RFID and how quickly the data is going to be purged from the system. And I think it's really important.

And I have to commend this Committee, in particular. I think that your recent work on commercial data profiling is showing that you're actually willing to say, "Well, wait a second. There's something that's perhaps a little bit bigger that needs a conversation here and that we want to play a role in addressing it." And I think one thing that is really important to consider is whether or not you might play a similar role here. You know, looking at US-VISIT is well and good, and I have to say when you look at -- from a process perspective, if you look at the State Department's consideration of the E-passport, which was, "Oh, well, we're just going to take the same data, and we're going to change the format."

Well, actually changing the format of the data is quite significant if you do any meaningful analysis of the security and privacy risks that it raises or if you even engage in any kind of threat modeling, right? You say, "Wow, that format change matters a lot." And if you compare that to what happened to DHS when they considered the US-VISIT program, they said, "Well, even though we're not going to make" -- "We're going to only use a unique identifier. We're not going to use the RFID to actually transfer information in the clear. We're just gonna" -- All of a sudden, you know, the State Department thought they were looking at an elephant, and the US-VISIT, DHS clearly thinks they're looking at a potential dragon, right? And I think the analysis that has gone on is quite distinct. And I think it's important for this Committee to kind of point that out at a large level and to highlight the fact that what we're basically doing in bits and bytes through various agencies is creating not what I would call a national identification system but what I would call a nationwide identification system that's going to tie into a far larger, global identification system, and that the consequence of that are perhaps a little bit easier for people to realize the significance than the consequences surrounding the US-VISIT program, in particular. So that's a little bit of history.

And I request that you continue to step back, which you've been inclined to do, and to think about the big questions, not just the little questions. So focusing specifically on the RFID issues in relation -- and I realize that's slightly broad -- but more specifically on the US-VISIT project, you know, the electronic passport comments that were provided to the State Department I think do a really wonderful job. Some of the comments were submitted by my students and myself, but many of the EFF affect, you know, (indiscernible) highlighted the issues around skimming and eavesdropping and cloning. And I don't want to go into that because I have other people -- I don't want to steal all their thunder. And I think some of the problems that were received on the US-VISIT program dealing with data quality and redress capacity are also very, very important in considering the appropriateness of this system. I remain a little bit puzzled about the requirements for the VISIT system. It was very clear to me that some of them are statutory, but then there are others where it seems like the shares in technology and business process should require no direct action on the part of the traveler. And I didn't really get that from any of the enabling legislation, So I'm kind of -- You know, it says that there's defined criteria, and I'm a little curious about who defined them because they clearly channeled the examination of the technology away from things like shooting bar codes and other things that are contact-based rather than contact lists. And, frankly, it's the contact list nature of the technology that raises many of the unique issues that we're dealing with today. And so I could go on at quite length, but I'm going to cut short there because my guess is that your questions are going to be far more interesting and illuminating than my rambling.

MR. ROSENZWEIG: Thanks very much. Your rambling was exceedingly illuminating. Mr. Tien, you're next.

MR. TIEN: Thanks very much. I'm going to focus on three issues: the privacy risks involved by new technology, kind of governing the issue credential, government decision-making accountability, and then the process by which TSA and DHS, in particular, decided to use on RFID, US-VISIT. I'm not going to discuss broader privacy concerns with US-VISIT than other groups have discussed in another forum. EFF is very concerned about the rapid growth of personal identification technology, not just RFID, biometrics, GPS, wireless, location tracking, public video surveillance cameras. All of these technologies collect more data about our daily real-world activities in a more fine-grained, high resolution way, often surreptitiously. I use the shortcut, location tracking. One friend of mine at Microsoft prefers to call it Student Inactivity Association. In either case, the idea is that you do not need to know what unique ID number goes with what person as long as you have a record that can associate events, transactions, whatever, with a unique ID number. It can be forensically or retroactively discovering or out-of-band in some other way. So there are two main risks here from a privacy standpoint. Obviously the leakage of content or skimming, learning someone's name, learning that a person is within the 3.2 million US-VISIT covered population. The second, what I just called the tracking, or Student Inactivity Association. And these can happen either via direct skimming or eavesdropping on an authorized transaction. And these are generic issues for insecure RFID tags.

The government-issued RFID credentials present some additional privacy policy problems. The first, in the short term, is simply choice. In the private sector, we may be able to decide whether or not to use a product that contains RFID. And even whether or not we can choose to do that, we may have the ability to kill the RFID tag in it once it has passed into our hands or merchants may offer that ability. If the government is placing RFIDs in passports or I-94 forms or driver's licenses, we're stuck. As we saw with the E-passport reg, you're not allowed to kill it. It would be invalid if you do. And for some government-issued credentials, like driver's licenses, many people will tend to carry them very, very often. The absolute risk of both information leakage, if there is information to be leaked, and tracking are high.

The next problem is more of a long-term problem, simply that government RFIDs are likely to drive the social spread of RFID. We do not claim that RFID is an immediate, right now, today, privacy problem because RFID readers aren't socially pervasive. The government employment of tags as information readers does push technology. By itself, it has more tags than readers. It also legitimizes the use of RFID as a tracking or other kind of technology, making it more acceptable to others or at least being ultimately inevitable, and of course it stimulates economic demand for RFID, driving down costs.

The third problem, of course, is that embedding any privacy endangering technology into the social environment threatens our social privacy. Using tracking technologies, putting government surveillance cameras onto street corners or facilitating wiretap and tracking communication, all of these share the feature of the government directly attempting to cripple private space or space that we all share in ways to facilitate the exposure of our activities. We have rules that tend to regulate penetrating or intrusive surveillance. We have not got a good framework of law or rules that regulates this sort of forced exposure. So, generally, the government needs the public to consider all of these potential effects on privacy when it makes decisions about using technology like RFID, which brings me to my second big point: lack of decision or accountability.

The GAO commented on this, and I've seen it in many settings, from rural school districts to city libraries to the State Department. There's simply a lack of public deliberation about whether RFID should be used at all and how it should be architected as it is. There is little advance public input in these institutions. Once complaints are aired, government entities are often reluctant to provide any reasonable justifications. In fact, they act offended that anyone would even be questioning them. Their deciding to use RFID is no more significant than deciding to buy new chairs. How can you, given the privacy issues, not act responsible? And what's really important is, people don't understand RFID very well. It's a relatively new technology in the wider specter outside of the public eye.

This means also that the RFID industry has strong channels in the government decisions with no privacy advocates or even mutual security researchers involved. When I listened to Mr. Westray's presentation about what they were doing before rollout, I didn't hear that, you know, the ACLU or EFF or EPIC or CDT or, you know, noted security researchers -- like Schneier, Boboon (phonetic), Wagner, Rueben, Wu -- consulted their work, but vendors were mentioned a lot. I'm also concerned that it's hard, therefore, for the privacy community or others who are simply concerned to get information about these implementations and how they work.

E-Passport is a good example. The State Department said that the PII on the RFID chip wouldn't be encrypted, and they wouldn't use the International Civil Aviation Organization basic access controls. And they claim that the chip could not be easily skimmed because the read range was short. But I don't know that, and neither do the experts I've consulted.

The government claims redress was only about four issues, but that's the spec for the RFID tag. Its intended read range, not the actual read range. Now, the media reported in this trial said that the read range at a distance of 20 to 30 feet. Some experts think it wasn't a skim, that it was just an eavesdrop. Maybe it was. The point is, we still don't know. The government hasn't said anything one way or the other about what the facts are. I never saw the State Department mention actual read range, and I don't even know before you ask them if there was a difference in the actual read range.

Where is the accountability here? You cannot expect privacy advocates to be able to rebut or to contest what the government does when both the government and the industry withhold any data they have about it that's relevant. And I don't know what they do, but I would think that if NIST was conducting trials on this, they would actually be there, but no one, as far as I know, has been able to see this.

So how does DHS's decision to use RFID in I-94 documents stack up here? I give them credit for using PIAs. That puts them ahead of the State Department. But when I look at the details, I'm still not all that satisfied. We know it will contain a unique ID number that will enable location tracking. EPIC has addressed those issues so I won't. But from a process and accountability perspective, the PIAs still lack details about the RFID implementation.

For instance, when I was invited to speak, I sent some questions out to find out more about the technology, because I couldn't tell from the PIA what was going on. So I learned that it uses the Nitrogen 15 megahertz frequency band. This wasn't in the public notice. Now, this is a band commonly used in other applications, with a high regrade of 100 to 1,000 PEGs per second, a read range of up to at least 15 feet, which obviously raises some surreptitious tracking issues.

I also learned that the implementation was proprietary, but I have no idea who the supplier is, what the protocols are. But Deirdre also mentioned the same thing I'm going to say next, which is I can't tell how this decision was made. We all know there was an operational change, and it was determined that passive RFID was the best for DHS's requirements, but I don't know where one finds that assessment. I don't know that privacy advocates or anyone outside was allowed to have input into that assessment or to poke into their criteria.

And as Deirdre pointed out, those criteria sort of drove the slope. On Page 17 of the PIA it tells us that GPS and active RFID were considered, but there was no mention of TP barcodes, etcetera. And that's because of one good criteria that was listed on Page 16: no direct action on the part of the traveler. That excludes a lot of options, but where did that really come from? You know, if -- You know, their requirements are one thing, but there's a prior question of whether those requirements are the right requirements.

Privacy advocates surely would have questioned whether a contact technology or an optional contactless technology would have been feasible. It's not obvious to me that that was ever asked. So the big-picture issue is, what sort of overall framework -- what kind of overall legislative policy types, is going to govern these decisions.

I said before that I thought that agencies were looking at RFID and, actually, the implementation of various privacy engagements and technology that's sort of no different from buying a desk chair. I think that's fundamentally, you know, the problem here. I do not want -- and this is not just at the Federal levels. This is at every level. I see city libraries. I see universities. I see school districts sort of decide, "We're going to adopt RFID" or "We're going to do this." And it isn't a single sort of overarching synthesis. There's no technology assessment. There is no accountability.

I don't want the DMV to suddenly decide that it's going to -- You know, you forget about realizing you're under any sort of Federal proposal. I don't want them to decide, "Yeah, we're going to put tracking devices into the ID cards" and then sort of leave that as a noncomplete, where 18 months after they've been working on pilot projects or whatever they make a public announcement and I have 60 days in which to respond. That's not the way this process should be working. You know, I just see a lot of individual agencies looking at their own requirements and not considering the sort of larger public interest.

So I'd like to see the Federal government take the accountability issues much more seriously. There should be full-fledged notice, comment, and rulemaking, inclusion of privacy advocates, as well as independent third party security researchers into this process in a way that creates a real record that can be questioned and allows meaningful evaluations. And that will, I hope, give the rest of the governmental entities all over this country, you know, some kind of a model, an example on how to do policy in this variant. Just Right now we have a real lack of policy. Thanks.

MR. ROSENZWEIG: Thank you, Mr. Tien. Good afternoon.

MR. NEUMANN: I'm Peter Neumann, and I'm somebody who's been in this field for vastly too long. This is my 53rd year as a professional in the field. I hardly endorse the comments that have been made by Deirdre and Lee. And in my position paper, in your handout, DHS-Relevant RFID Related Risks, I enumerate a lot of points that have not been made. I would hope that you will all have read that in some detail. I would like to try and pick up some points that haven't been made previously.

The first is: Beware of technological solutions in the small to problems that are not just technological problems in the large but involve a great many concepts and a great many people and a great many people in critical positions where you're relying on them to do the right thing at the right time under extremely difficult circumstances. So the first point is really: Look at the big picture.

Deirdre did mention that, but I'm going to look at it in a even bigger picture. I'm often related, called the designated holist, and it certainly works out in this particular session. The big picture recognizes the fact that the technologies themselves are flawed, whether it's RFID or biometrics or whatever. The operating systems in which all of these things are embedded, in the sense that all of the databases and networking and encryption and everything else, are fundamentally flawed.

What we have today is an infrastructure of computer systems: PCs, and laptops and everything else, wireless little hand held things. The networking, which is fundamentally subject to subversion and denial of service attacks, the cryptography, biometrics, all of this stuff has very serious technological limitations and has serious problems involving the human beings who are expected to do the right thing all of the time.

Now, RFID requires not just an understanding of the technology but the way in which all of this is embedded into the total system concept. Border crossing, which U.S. has to address, is one of the problems. Airports are a border in a sense. You're going from an unsecured area to a supposedly secured area. You have to worry about whether all of the FedEx folks and the UPS folks are going through the same procedure. They're not, typically. The forgeability and masquerading of identities have to be considered.

I have a bunch of points. Let me try and make a quick pass through a few of them before I run out of time. DoD always likes to look at the concept of strength and depth. What we have is weakness in depth. Everything is essentially a weak link in the technology and all of the surrounds. People are, of course, an enormous weak link. Insiders. We've seen a lot of problems with insiders who -- Systems are built with the assumption that everybody inside is trustworthy, and that is a very bad assumption.

There are technological flaws. Back in the days of Clipper escrow, there was a very simple attack that completely defeated the entire escrow mechanism. This was a secret algorithm. This was a process that had been supposedly vetted by the DNSA and yet had a fundamental flaw. The same is true of some of the wiretaps. I think we're going to see some new results in a week or so, if they haven't broken yet.

Technology has fundamental limitations to it. And so I've outlined in my written documents, or pages of text, a large number of the limitations of RFID technology, of the risks of some remediation techniques that might be taken of the importance of research. I find that in this particular environment in which we live, whether it's funding from NSF or DARPA or NSA or Homeland Security, who is actually funding my having written this document, that the concept of fundamental farsighted research has been lost, almost completely, in the large-scale system sense.

There are little beautiful pieces of research, for example, relating to cryptography. But the embedding of that cryptography into large systems doesn't seem to be a problem that anybody's worried about. So I say in my paper -- it seems self-serving for somebody with a life-long commitment to research to be saying -- there is a problem here because the way in which research is being dealt with in this country is seriously short-sighted. But in terms of the RFID technology itself, it is applicable in low-threat identification. It is not applicable in high-threat authentication. They're finding between the tag and the actual entity that is supposedly being tagged is very subject to masquerading and all sorts of things.

If you throw in biometrics, the biometrics have some serious problems. You must remember that a false-positive rate, a false-negative rate of 1 percent when you're dealing with, say, a million people is still 10,000, and you can't deal with 10,000 inceptions in realtime. So relying on that technology is a fundamental problem. And all of the systems that I've seen that use technology like that ignore completely the people who are administering the system. If you look at the problems in going through airports, there's very little real deep understanding of what's going on by the people who are administering it.

A couple other comments. The technology is inherently subject to subversion through replacement tags, through denials of service, jamming, disabling, and so on, irrespective of the implications. Many of the would-be terrorists are not inside the system. They're not known in the system, or they're masquerading as people who have legitimate identities.

Even with the very high-powered RFID tags, the large memories, many of the risks that we're talking about will remain, and there are a lot of serious problems. So I think we have to look at this problem not just in the small for one particular kind of use of RFID tags but much more broadly; as has been suggested, all of the identity authentication problems.

We have the mission creep problem where the Social Security numbers are being used by banks as authenticators. Any use of an identifier as an authenticator is seriously misguided. And I would say that the most important thing here is really understanding the concepts in the context of the big picture. Since you guys have talked about EFF, I should throw in the quote in the end of my thing from the EPIC comments on US-VISIT, which said, "DHS should have been in the use of RFID technology because of security and privacy threats. The proposed RFID implementation lacks basic access controls. DHS should not permit routine usage for an RFID application to simply intend to automate the process for entry and exit."

There are a lot of problems, and by just focusing on, say, border crossing or airports or anything like that, you're missing the boat. And I believe that you have already demonstrated, to me at least, that you are very much interested in the big picture. As one indication of a research paper, I refer to the paper by Ari Juels, David Molner, and David Wagner, security and privacy issues on E-passports, and that's available on their website. It's presented this month at the security conference, and it considers RFID tags and biometrics, security for RFID implications and E-passports, and many references to what is known in the research community about what works and what doesn't. I also include a few references to my own writings on understanding the risks of technology, understanding the potential misuses of technology, and the consequences of those misuses. And I think those misuses are pervasive.

If we look at the way in which technology has been embedded in systems in the large -- Just about every system I've ever looked at had some serious problems with it. If you look at these specific problems, you discover that we keep making the same mistakes, over and over and over again. As one example in Internet security problems, buffer overflows have been around for many, many years. We got rid of them in 1965 in the Multics system that I was part of the design and development team for. We understood the problem. We had a solution and completely avoided them. The technology today keeps making mistakes, over and over and over again, and we can expect that the ways in which RFID technology will be embedded into systems in the large will continue to make many of those mistakes. Thank you very much for the opportunity to be here today.

MR. ROSENZWEIG: Thank you. To the panel, a couple quick notes. You'll be pleased to know that the Juels, Molner, and Wagner paper is in our briefing books already, so we don't have to go to the website. So at least we are doing the right thing in trying to put together information for the Committee. And I'm going to exercise my privilege and ask the first question, since I get to call on people, and though I take very seriously, Ms. Mulligan, Mr. Tien, Mr. Westray, the idea of stepping back, and that's certainly one, I think, we want to press upon in the long run. I'm going to ask a really narrow, specific question for Mr. Westray just because we came and we saw this project in operation yesterday up at Bellingham, for which we're very grateful for the time and energy of all the CBP people there. I hope you'll tell them that. But in your testimony, you said that the I-94 RFID was linked to the passport which contained biometric information upon entry. My understanding from yesterday is that there's no such linkage on exit, so that at least as currently designed in the proof of concept, the only thing we know is that the I-94 form has left the country. And while presumptively it is being carried by the person to whom it was issued, that presumption is imminently falsifiable, in that I can, at least as currently designed, spoof the system simply by giving the I-94 form to my friend Lisa who's going out of the country already, and it will look like both of us are leaving, when only she has left. So my questions are: Am I right in my understanding of the architecture of the system now? And if I am right, what, if anything, does US-VISIT intend to do to fix that architecture, or is that something that you plan to build in and accept because other alternatives are too costly or ineffective?

MR. WESTRAY: Well, I'll say it, and maybe I need correction here. The unique identifier is not linked to a passport. Just the biographic information is selected upon issuance.

MR. ROSENZWEIG: Fair enough. I'll take that amendment as linking it to a specific individual but only upon entry, at least as I understand. What is their linkage on exit?

MR. WESTRAY: On issuance. And you're right; there is no linkage -- Well, there is a linkage for exit, but, again, it can be spoofed if, in fact, you were to hand your I-94 over to someone else for exit. Now, understanding that there are some that say, well, we're getting much more information than we currently had and also understanding that RF technology is emerging. And we all understand that this isn't the end-all, be-all technology, and we're always open for bigger and better and to push industry for solution-based technologies. But you're right; there are some holes in the system and we're aware of them. And, again, this is a proof of concept.

MR. ROSENZWEIG: Would it be the intention of US-VISIT to plug that hole before deploying this system?

MR. WESTRAY: Absolutely. Absolutely.

MR. ROSENZWEIG: Do you have any idea or can you share with us any indication of how that might -- what things you're considering for hole-plugging on that particular point?

MR. WESTRAY: Well, our business owners are looking at ways in which we can do that. We're working with Customs and Border Protection. There were discussions about implementing an outbounded tollbooth, where we can put officers on outbound to do checks. There's also been talks to work with the Canadian and Mexican governments, that their entry be our confirmed exits. So, again, we are looking at different strategies in which we can show -- Again, we're very aware of the holes in the system.

MR. ROSENZWEIG: Thank you. Keeping with our practice of those going first who haven't participated yet, Kirk.

MR. HERATH: Thank you, Mr. Chairman. I want to thank all of you for coming today. I have one -- I guess it's a major question. And you've all -- the nongovernmental speakers have spoken to this in some way.

Mr. Tien, you spoke to it probably most specifically, and it's something that I think we grapple with as we look at some of these thorny issues. Exactly how much detail would be necessary to adequately assess or analyze privacy and security risks? I mean, I -- There's got to be a tipping point to where too much detail raises security concerns themselves. And then you also have the issue of who is adequate to participate and who is legitimate in your eyes to participate. You know, obviously, we can't have complete transparency about everything to everyone, but it does -- you know, it's something that I think, as I wade through the book every three months and as we listen to panelists, it's a reoccurring question or concern. And we have had Mr. Oberman here several times and posed significant questions to him, and I still feel like I am missing things. So it's a large question.

MS. MULLIGAN: I'm going to grab the mic first. It's a really important question. Peter Neumann and I and several other really prominent computer security and other kinds of researchers recently got a large National Science Foundation grant to look at voting systems, right? And there's a similar problem there, right? As we enclose systems that used to be transparent. All of us were able to look at the ballots and see what's going on, and all of a sudden the ballots become something that's in this box and the code is proprietary and its people -- people who go to the polling places can't evaluate it and the Secretary of State who's buying the machinery doesn't really know what's in it. And so you have the same closure of a process that used to be really transparent. And it -- I mean, your question is incredibly important.

How as a Committee, how as a public, how as government officials can we exercise the oversight and accountability that we need to in order to assure that our machinery is adhering to whatever values we decide we need to build into it. And I think the answer is -- I'm not completely sure what is required completely, but I can tell you what's happening right now doesn't work. And I'll give you an example.

When the E-passport regs came out, I was incredibly troubled by the lack of information in them. Right? There were statements such as, "Encryption is too expensive." I was like, "Well, that can't be true." "In encryption, there's no national standard." I'm like, "Well, I know that." There was absolutely no data backing any of the assumptions, and if you just think about the kind of statements that we require about economic consequences of a regulation, you know, it didn't even meet that standard; there was just no data provided to back up any of the assertions that were being made. And I think that the US-VISIT program, you can -- I had no idea what standard of RF technology they were using. How can anyone evaluate technology without even knowing anything about its fundamental properties? And the answer is: You can't do it and the public can't do it. And there's no meaningful oversight, if that's the case.

So in the context of electronic passports, I actually have a whole binder full of documents about the NIST tests that have gone on that I had to FOIA. Right? But in order to get enough information to make any kind of assessment about whether or not they engaged in the right kind of testing, whether or not they engaged in the right kind of threat modeling, whether or not the technology -- what kind of analysis they did, and as far as comparative analysis across technologies, what were the guidelines established for functional -- just functional testing, let alone security testing -- You know, none of that was made available in the public documents. So in addition to doing that I said, "Okay, well, if they're not going to provide some data about their own testing, I guess we have to do our own." So my students and I have been -- I have spent the past six and a half months just trying to get the chips, right, and trying to get the readers in order to do any independent security testing of this technology. And if the government isn't going to provide it and if people aren't going to compel that that information's provided so that independent experts, security experts, whatever, can analyze it, I think it's deeply troubling that we can't even get the technology outside of the government ourselves. And I'm not saying that we should have managed to pull that all together, but it was at enormous length. And I think your question about how can we reliably analyze this is one that's incredibly important.

MR. TIEN: I am going to add onto that. I am a FOIA lawyer. I used to litigate Freedom of Information Act cases. I've asked the Federal government against the National Security Agency, the CIA, and the FBI. My experience -- So you can understand, I'm very biased. My experience is that they routinely obfuscate, lie, and really don't give an honest explanation to the public about why information needs to be withheld. I would say that the most corrosive thing for this Committee or any one other body to do would be to assume that presumption of closedness is necessary. You have to have a presumption of openness because the government agencies, whether it's because they have a misguided notion of security or want to protect the proprietary interest of vendors that they talk to or don't want to be embarrassed for one reason or another, if you assume that they are acting in good faith about not wanting to say something, you are just going to create a culture of closedness that makes any meaningful oversight impossible.

The burden must be strongly on the government or on the agencies to explain why something cannot be disclosed and not the other way around. I have found, unfortunately, judges would often do the government's work for them by hypothesizing or speculating what bad things could happen. But the fact is, in time, case after case, when judges order disclosure or when information comes down, the parade of oracles does not occur. It's extremely unusual. I have had cases where I was able -- through sort of, essentially, private research -- uncover what it was that the government did not want to disclose. And it was really quite innocuous. There is a great deal of obfuscation, and I think it really, really hampers any kind of oversight.

Now, I also want to say that I think there are problems with this sort of a staged, staggered approach which we see, say, in the situations where information is disclosed to Senate Intelligence but then Senate Intelligence can't disclose it further. You end up simply pushing the problem around, you know, like a pillow into a different place, but ultimately it does not get to the public. I think the one thing that has to be understood is that there is a real perception problem, often, inside the government about what the deleterious effects of disclosure will be.

And I'm really -- I guess what I want to say is, I think that a lot of times in thinking about, "Well, it will be bad if people learned about this," it's often based on misapprehension of how people react and what they already know, especially people that you're most concerned about, because a lot of times, it will be "Well, we're not concerned about them. We're concerned about the bad guys. What if the bad guys knew?" But how do we know that the bad guys don't already know? And so assumptions like that just skew and bias any kind of attempt to create openness in this area.

MR. NEUMANN: Let me remind us that the Committee's name is related to privacy and integrity, so let me broaden your question and paraphrase it, which is, really: When are the risks to privacy and integrity too great? And this is a slippery slope. I'll give you two examples. You mentioned the voting problem. The electronic voting systems in this country that are supposedly certified for use in our elections in the past few years are designed against archaic standards that are fundamentally flawed in a design process that is proprietary; they are evaluated in a proprietary process that is paid for by the vendors; and, essentially, there is absolutely no way of doing a recount or an audit trail because there is no audit trail and there is no assurance that anything works correctly. So this is one extreme example of a very bad technology situation, which when you look at it in the big system problem, you have the registration problems; you have all sorts of other things, all the way through to the final tabulation.

The other is the identity theft that can result, not on a slippery slope small scale, but can result in the massive scale, where you discover that the database backup records of entire financial systems are lost as backup tapes. You ask, "Well, why weren't the backup tapes encrypted?" And the answer is, "Well, the key management problem is so difficult that we can't encrypt them because we would never be able to recover the key so that we could recover the data."

And, again, it's a human interaction with a technology that has serious limitations. So those are just two examples of the kind of slippery slope that one sees where one says, "Well, in the small, everything works just fine, but in the large, it breaks down enormously."

MR. ROSENZWEIG: David.

MR. D. HOFFMAN: Thank you, Paul. I'd also like to thank the entire panel for being with us today and, specifically, to thank the nongovernmental members of the panel for their legal and technical scholarship in this area over the long term and recently, which has proven extremely helpful for us to think about these issues. And I would ask you also to continue to explore these areas, specifically the scholarship in the areas of legal and technical areas, specifically around, "What does it mean to have a reasonable expectation of privacy, especially in public places." And I don't think we've explored that much as a society, and I think some of the technological development calls for us to have some very robust discussions about that. I also think what we really could use is some scholarship help in doing case studies of exactly how do you think about noticing things with some of these technologies, which I think would really help the folks who are trying to deploy them. And -- I'm getting to my question.

In that line of case studies, it seems to me we're not always being very coherent in the way we're talking about what the risks are to the individual from the technologies. We talk about grants, visions, but specifically with this particular technology, it seems to me the risks -- We've talked about several risks, but the primary one has been this idea of skimming and that people would be able to read the tag in other places. Wouldn't one effective way to take care of that be to just employ some low-tech solution, like a Faraday cage, to block the emission, and if that is the case, shouldn't we be recommending that strongly? And I'd like to hear from Mr. Westray whether that was pursued or thought about as a potential alternative to make sure that this couldn't be read after the person is passing over port.

MR. WESTRAY: We did look at several alternatives. And, again, we really didn't want to put a lot of burden on the traveler in terms of metal or aluminum shielding, so forth and so on. We have had an extensive outreach effort thus far to really let the constituents know of our desire to mitigate privacy concerns. Again, we're using passive RF technology, which has to be awakened by a reader, so it's not emanating all the time. I'd also like to say that this isn't an inspection replacement technology. It's just used for inspection enhancement technology. So even as the traveler approaches the border, the officer will still look at travel documentation, look at their Visas, look at their passports. But, again, our goal was to provide that officer with more information to make an admissibility decision. Again, it wasn't to say that RF is the end-all, be-all. We just wanted to provide more information up front to help facilitate the inspection process and save some time. I kind of ventured off a little bit, but those are some points I wanted to make.

I've written some other points down. We feel it's pretty noninvasive. Again, it's passive. There's not much traveler interaction. It's a unique identifier to the user, as I said it before. Our software was designed -- This answers another question that was raised earlier. The software is designed to seek a tag range. We have a specific tag range. So if, in fact, a tag was remanufactured or recreated, again, when that individual that has this tag comes into the border, my photo will pop up on the screen in front of the officer, as the person who is the owner of that tag. So, again, I think we have put some security measurements in place as well.

But, again, I'd just like to reiterate that this isn't, I don't feel, the end-all, be-all solution, and we're always open to privacy concerns and bigger and better technology that's out there.

MR. TIEN: If I could quickly comment both on your question as well as Mr. Westray's answer. One of the big-picture issues -- it's not as big as, you know, ID in the first place, but at least in the choice of RF technology as a technology at all is that, you know, RFID has this property, whether passive or active, of being -- as I like to put it: It's not secure; it's a promiscuous tag. It will talk to any reader that is able to -- that is within range of the frequency. And you don't know that this is happening. So I understand the motivation behind the idea of a Faraday cage, because I've been working on a bill in California that would govern government-issued ID cards containing RFID, and that's something that people come up to us all the time about: "Well, why not just use Faraday cages?" But I think Mr. Westray pointed out on one the issues that it requires the person carrying the item to do extra things to protect his information -- his or her information or his or her unique ID number from being surreptitiously captured by unauthorized RFID readers.

And as Senator Simitian, who is the author of our focus group, posed, should the burden be on the citizen to protect him or herself against being skimmed or trapped when it is the government that is putting that technology in -- and requiring that to be in a credential that they're carrying. There is -- And if we know or if we believe that it's the tendency of people to forget that this happened, to not know that this risk exists, then you are really saddling people with an absolutely unnecessary burden, especially in the situation where it's not even a necessary replacement for people --

MR. D. HOFFMAN: Could you just tell us in detail what that burden is and what those steps are that would be required of the individual?

MR. TIEN: Actually shielding it themselves?

MR. D. HOFFMAN: Yeah. I mean, I'm assuming that there is an alternative where the government could provide the shield.

MR. TIEN: Well, for instance, the discussion of the E-passport, there is the idea that because the E-passport is in a booklet form, as opposed to a card form, that the actual cover of the passport will contain metal and other fibers sufficient to shield or protect or prevent the RFID tag from being read. If you were to have the RFID tag itself in a, say, standalone driver's license, then you would need a sheathe of some sort, a bag of some sort, or a wallet that contains shielding material or a purse that contains shielding material in order to secure it.

We had a funny incident in California where we use on our ID at the -- CalTrans uses for RFID for the Fast-Track toll booth, so apparently they issued Mylar bags to everyone carrying a Fast-Track pass so that they could -- when they weren't actually needing it, to go through the toll booth. They could put it in the bag and keep their tags from being read. But, of course, most people actually physically and permanently affixed their Fast-Track cards to the dashboard or whatever, so they end up apparently not shielding it at all.

And then we've now heard reports that the bags may not actually shield as expected in the first place, that they don't actually work. I don't know whether that's true or not. But, again, it is sort of along the lines of, you're asking the person to take precaution, and you're asking them to verify whether or not the precaution works. And all of this is sort of, in my view, kind of like trying to make water not wet, right? I mean, when you use promiscuous RFID, it is like water, then all of these mitigating measures are trying to get it so it's like a contact card. Well, why not just use a contact card in the first place, unless there is a truly compelling reason, which I have not seen.

MR. ROSENZWEIG: Unless somebody feels really burdened, I think I'm going to draw the line under who's here, which will take us into our scheduled lunch hour. That is, I'm going to let people whose tents are up ask, and unless somebody really burns, that'll be it, okay? Ramon, you're next.

MS. MULLIGAN: I have one quick comment.

MR. ROSENZWEIG: Well, you know, you're just extending your own time here, and all of us, before we go to lunch, but go ahead.

MS. MULLIGAN: I'll be really quick. I completely agree with you, David, and Lee highlighted this in his opening remarks. The question of how we deal with privacy in public places, which is something that we have really avoided, is probably the most pressing question facing privacy today, and I think you should view the question about installing RFID technology in this particular application in the broader sense of what is the sensor network fully wired environment that we're going to live in look like, and how will this particular piece of paper with this particular piece in it interact with that whole system? And it's not going to be the Mylar slip; it's going to be the mylar coat that's going to be issued, right?

MR. NEUMANN: I just wanted to respond to your question itself, not an answer to the question, in which you focus on that particular privacy issue as very important. In my printed -- my handout, I identified ten different integrity issues that you want to look at. And, again, putting on my hat as designated holist, it is the totality of all of these problems. It's for you to decide what the relative risks are. I identify a lot of integrity issues, and I think these are very important in this context.

MR. ROSENZWEIG: Now, Ramon.

MR. BARQUIN: I have one comment and one question. The comment -- And I truly appreciate the different testimony from our distinguished panel, and it is extremely important that we be able to do the kinds of research and the kinds of activities that you have suggested as we move ahead. I am concerned with this issue of -- going back to Raymond Bower who said that the most important factor of man's total existence was the ability to identify as early as possible and correct the unexpected, undesirable second-order consequences of technology. The problem is, that is very, very difficult to do. We've got to try. I mean, otherwise, we would have killed the internal combustion engine because of the potential for pollution, etcetera, etcetera. The biggest issue here is that I detect that we are now just having a very, very significant gap between ourselves -- the people and our government -- in terms of the relationship of trust, and unless we find a better way of dealing with that, we going to be, I think, moving very, very much in the wrong direction.

Now, that leads to my specific question, and it was for Mr. Westray, because in addition to all of the concerns raised for privacy, the question of efficiency and effectiveness of the technology vis-a-vie what US-VISIT is supposed to be about, is the one that really is very much in question here. Yesterday we saw, for example, how the CBP officers worked using the I-94s, and we asked the question, "Are you gaining any times? Is it any different when the officer actually swipes the password?" And they were very, very hard-put to say that they were getting any time at all. But I'd like to really understand how deeply you looked at the question of efficiencies and effectiveness vis-a-vie the US-VISIT and RFID.

MR. WESTRAY: Well, I think I can better answer your question when the evaluation is fully performed and I can have complete evidence to support or to not support this effort. I do feel -- and you visited the location. We had a reader in the doorway upon entry, so we were able to capture these reads even before they approached the booth. It gave us some considerable amount of time on the back end to do watch list checks and stage information for that officer so it wouldn't be the traveler approaching the officer, a subsequent second read would take place, and they pull the information up, so I do feel that they are gaining a lot of time, which would have been spent in front of the officer, that we're getting even beforehand now. So, going back to your question, it will be better to gauge that when a full evaluation has been completed on this.

MR. ROSENZWEIG: Mr. Westray, in the past DHS witnesses have agreed to answer follow-up questions from the Committee. Would that be an acceptable forum for you? Can we send you a question --

MR. WESTRAY: Absolutely.

MR. ROSENZWEIG: Excellent. Well, since you were here this morning, you know that I also note when people don't answer them, so I'm hopeful you'll be -- you won't be named in December. And, actually, since I'm on this, there are fewer typically for the nongovernmental witnesses, but if there are for you, may I send them along to everybody?

PANEL: Of course.

MR. ROSENZWEIG: We'll collect them and see if there are any for you folk.

MS. MULLIGAN: Can we get the answers?

MR. ROSENZWEIG: Oh. Just so it's clear, our questions and answers are all posted on the DHS privacy Committee website. You've got to go through a couple of buttons, date of the meeting and so forth, but when we get them -- This is a learning function for us and a transparency function as well. So far, there haven't been any that we haven't posted. Next on the list is Joe.

MR. ALHADEF: Thank you. And I'm almost reluctant to ask my question because this is a little bit of a follow-up to David's, and I don't want these questions to be a disincentive to speakers coming because we're asking you to do homework now. But essentially, Mr. Tien kind of gave us the why the policies aren't working, and Mr. Neumann pointed out in a very clear and detailed fashion in his paper, you know, what are the limitations on the technology side with some concepts of how you might remediate that, but realistically only if you use it in the low-risk environment. And I'm kind of gathering the fact that we see a lot of scholarship in both of those camps, but we don't see scholarship that talks about how the policy remediation and the technology remediation can work together to get us an acceptable space. And I was wondering if you guys know of whether there is such scholarship out there or, if not, who might be working on that, because I think the question is: Both processes seem to be broken. We may be able to fix both of them to a certain extent, but can we fix them in a complimentary manner so that the parts become greater than the whole?

MR. NEUMANN: There are a couple of examples, which I will throw out. From my own laboratory back in 1973, we did two things. We built a very secure -- or designed a very secure system for NSA, and we built the world's first fly-by-wire system for NASA. Each of those had a detailed, formally specified set of policy step and formal specifications of the design of the system and, in some cases, formal proofs that the design was consistent with the policy and, in some cases, the code was consistent with the specifications. In the research community, there's been a lot of work on formal requirements, specifications on -- formal design specifications, and the ability to map and model and do some consistency proof to show that the one thing is, in fact, consistent with policy. In the real world -- That's in the research community. In the real world, this never happens.

MS. MULLIGAN: It's certainly what I do for a living, is try to put those two pieces together. And to give you some specific examples that I think are relevant, given the read range of these particular chips -- potentially they're not completely relevant -- David Molner and David Wagner -- who are the two of the folks on one of the technical papers you have -- myself, two of my law students, a Ph.D. student in engineering and computer science, and two of my law fellows worked together to both give advice to the Berkeley Public Library on their implementation of RFID in the library setting, to provide guidelines and best practices in the use of RFID in the library setting, to do a threat analysis, and to provide kind of very specific advice. And we also offered to referee a scientific paper for a scientific conference on that particular issue, and so I think there are opportunities to do that.

I think the demise of OTA really limited the instances in which it happens within the federal government. But there are folks in the research community that have recognized the need to actually do technology policy. And the voting center that we talked about, another research grant that NSF funded recently when I was member, where I'm looking at privacy and public places is dealing with ubiquitous computing and security and privacy issues. And that, again, pulls together social scientists and engineers and computer scientists, but I don't think that that kind of research -- I don't think that sound science and technology policy often enough inform federal policy making. I think there still remains a gap, and I think, really, the largest reason for that is the OTA's shorter lifespan.

MR. TIEN: My perspective is slightly different. I agree that this is a very important issue to be worked on. What I've seen is that when you do get good research, like the kind that Deirdre has done or has contributed to, it is often because of the kindness of strangers. For instance, you know, when I -- in working with David Neumar (phonetic), for instance -- you know, he's got personal connections with people in the industry. They like him. They'll talk to him. He'll be able to get a hold of things that are necessary in order to do something scientific. But there is no systematic means by which anyone can pry vendors or industry considers to be valuable business information in order to do a scientific study. Even large companies that have large research departments aren't always very free to talk about the issues that play their technologies. We see this in the biometrics field. We see this in the RFID field.

I mean, to be really honest, there is a big money issue here, right. Like, companies are running around trying to tell Congress that "This is the best thing since sliced bread" or that "The agency should use this" or... I mean, right now, all summer, there have been working groups inside of DHS trying to decide what machine, what readable format should be used in the Real ID, whether optical or whether RFID, whatever. Millions and billions of dollars are on the table here, and working in California on the RFID bill, the American Electronics Association and the other technology groups coming in and will, you know, just make a lot of statements about their technology. They're impossible to verify.

So I think the most fundamental problem in this area is not that there aren't researchers who aren't really interested in figuring these problems out, or that there aren't privacy and public interest groups and law professors who are interested in figuring this out. It's that at the end of the day, much of the information that you would need and much of the will and commitment that you would need to move in that direction is actually in the hands of either private sector businesses or government agencies who don't have any particular incentive to move in that direction. So I don't know how you cure that structural problem.

I complained about not being involved, for instance, or not being able to be involved in some of EPC Global's decision-making, where they -- you know, where I attended an NAS meeting about RFID policy, ubiquitous computing. And I said, "Well, you know, the specs, it's really hard to get to these specs." And, you know, "We're working on our technical capacity," you know, "software people on board and we talk to experts all the time. But we're not getting involved." And what I heard from one of the folks there was, "Well, it's easy. You just have to pay a membership fee." You know, $10,000 or whatever. "And you'll be flying to meetings from here, there, wherever, and you'll be able to fully participate." My organization cannot afford that. The only reason I'm here today is because DHS is paying for the air fare and the hotel. If they don't pay, I can't go anywhere. I mean, it's just that simple.

MR. ROSENZWEIG: We're paying? Joe, quick follow-up.

MR. ALHADEF: Yeah, one that doesn't require a response. In terms of what would be most useful to the Committee is if you could suggest some resources that would help us frame the thinking that we're doing on where those two issues may be most mutually reinforced and what kind of analysis framework to use and evaluate them together, as opposed to separately, that would be great.

MR. ROSENZWEIG: That suggests that you're getting a follow-up letter.

MR. HARPER: There are more follow-up questions, but a yes-or-no question for MR. Westray, with a very long preface. Sorry. I do appreciate all of you testifying today and coming to speak with us. And much of what you've said jibes with my thinking on these issues. In particular, Professor Mulligan, I felt that wind that's blowing everyone toward RFID and don't know the source of it. I'd like to know the source of it.

MR. ROSENZWEIG: Jim.

MR. HARPER: The RFID tests are excellent questions. And this test seems to be following the same pattern as E-passport, which will have an RFID tag in it but have no particular benefit over the old passport. And, in fact, the I-94 might be a detriment on a number of different vectors. And, Mr. Tien, likewise your points about transparency are extremely well-taken. And in that vein, all these veins, I'm interested in learning about the business, about the RFID supplier business. So, I wonder, Mr. Westray, if you could provide the contracts, documents, whatever it is, that will tell us who is making money, which providers of RFID are selling this to you and what they're getting for it and those kinds of things so we can understand what the business model is and how it works.

MR. WESTRAY: Absolutely. Right now, Customs and Border Protection have a few RFID programs out there. I'm sure you may have heard about the Nexus, SENTRI, and Fast programs. These are trusted traveler programs. It involves an enrollment process. Travelers pay a fee. They get a dedicated commuter lane because of it. They get a proximity card. Upon approach of the officer's booth -- which is, again, a dedicated lane -- you display your card, your tag is read, information is displayed for the officer, and you can move forward. We decided to use the I-94 approach because we didn't want to put another form factor out there. Again, the I-94 was already being used, and, again, travelers could have up to five, six border crossing cards. And we didn't want to bombard them with another document, so this is why we used the I-94.

MR. HARPER: The key thing is, obviously, the information about which companies provide it. So if we could get information after --

MR. WESTRAY: Oh. Certainly.

MR. HARPER: Thank you much.

MR. L. HOFFMAN: Thank you and thank you all for coming to talk to us. I'm struck the more I listen to panel comments how they echo comments made at our Boston meeting by Latonya Sweeney, professor at Carnegie Mellon. We specifically asked her, and it's in the record, you know, "Have you tried to get money for research on privacy?" She basically said "Anything with privacy on it is dead on arrival at the DHS research office and at some other research offices as well." So I especially commend some of the panel members in getting their grants to look at things where -- In building systems, in particular, which I know something about, I'm concerned that we don't go down the same road that the elected officials or appointed officials have gone in voting systems, where, in essence, you often have a group of paperless voting systems. Some people have said that the -- you have the rapacious selling to the clueless, or something like that. I don't want that to happen here, and I do have some concerns about that. I have a more process-oriented question, and you can either answer now, or if you have comments you want to later send, I and the Committee would welcome them.

What changes would you recommend in how DHS does its research, how it funds its research in it's large directory, looking at that, what it looks for, if it is not holistic enough, if there's too much attention being paid to "Let's develop this new toy and get it out there" and not enough attention being paid, as I think some of you think, to where this all fits together. How do we do that? Do we try to incent people in some way? And if so, how? Do we try to use set-asides to compel them? In particular, what changes in process do you suggest before implementation? I'm concerned that some of the programs I've heard about, today and other times, people just start running along, running along, and running along, and then the right questions get asked, but the program is half done; and then people say, "Oh, it's only a test," and they've spent a lot of money, where, you know, you can spend a lot less money and do it right the first time if you ask the right questions.

MR. NEUMANN: I guess that question is for me in that I am working currently with Doug Maughan, who is in the Science and Technology Division of DHS, and we have established, under his contractual arrangement, a cyber security R&D center. We are actually helping him in developing various programs, including very specifically, despite Latonya's comment, several things that relate specifically to privacy. In fact, the PIA that was on the street up until a few weeks ago, few months ago, had a major section on privacy. The problem has been that the money that is supposedly earmarked for not just privacy but cyber security has continually been reprogrammed for chem and bio-nuke, and the DHS as a whole, up until the point that somebody decided that we need a deputy director for cyber security and integrity and privacy, and so on, up until that point, has been that there is no problem relating to cyber security.

We've never had the Pearl Harbor, the tsunami, and the Katrina, whatever, of cyber security, of that magnitude, and therefore, it's not a problem. Now, I spoke before the Marsh Commission for Clinton's critical Infrastructure Protection Group on five different occasions. Each time, I told them -- again, wearing my hat as designated holist -- that the problems were much bigger than they realized. Each commissioner was looking at his own scope by the railroad guy, the one in telecommunications, the gas guy, the electric lady, and so on. And they -- none of them really got the fact that all of this was connected. Everything is on the Internet today. This is the worst thing of all because it's all totally vulnerable.

All of our critical infrastructures are vulnerable. And the commissioners never really got that message in all of the years of that Commission. So I think the problem in Homeland Security, in direct answer to your question, is that apart from Doug Maughan, there's no one in DHS who really understands -- and I hope you get him to talk to you at some point. There's no one there who really understands the way in which the cyber security and privacy issues completely underlie absolutely everything that they're doing. Is that an adequate answer to your question?

MS. MULLIGAN: Could I add one little piece to it? I am speaking from lack of complete knowledge, but certainly my understanding from the computer science community is that there's been a real -- and you can probably speak to this better than I, Lance. There's been a real shift in federal grants generally away from long-term and deeper thinking about science and technology towards much more short-term, quick-to-market proposals.

And at a very fundamental level, that's exactly what we don't need funding for. Right? Business is good doing that, get it to the market. And at that point, it's actually too late, right, to talk about social values. So, you know, it's the voting system talking about equality and equal participation and privacy and security and transparency that has to actually happen in the design phase so those things can be embedded. It can't happen when you have projects built and you're trying to figure out how to retrofit. And I think that the shift in funding priorities has meant that it's much less likely that the kind of values that your Committee is aimed in looking at are going to be adequately reflected in the research process, because that's not where the funding is going.

MR. NEUMANN: In direct answer to your question, DHS is probably in the order of the magnitude worse than DARPA, which has definitely gone in the direction of classified projects, and very, very development-oriented, but not research or needed, certainly not long-term research.

MR. TIEN: I have a very short point to add.

MR. ROSENZWEIG: Yes, please. At the risk of terminating this, our next speaker leaves on a plane at two.

MR. TIEN: Congress is a huge part of the problem because Congress legislates a program and then expects an agency to implement it according to social values and also puts it into a double blind, where it cannot actually do that. And they are -- I mean, we saw this in biometrics -- ordering biometrics screening, and I saw agencies at GAO workshops complain, "Well, we were told to do this, so we have to. But this is insane. It's very hard."

MS. MULLIGAN: It's not a biometric.

MR. TIEN: They're asking something that they really can't do well.

MR. ROSENZWEIG: To be honest, though, I think the congressional problem is outside the scope of this Committee.

MR. TIEN: Yes. But it's important to recognize where the problems really are, because they try to fix other things, and that's the problem.

MR. ROSENZWEIG: Howard, you get the last question, and then we're going to have to run to the classified area.

MR. BEALES: I want to go back to the big-picture focus from the beginning of the panel. It seems to me that -- and I guess it seems to me the starting point has to be: There are no perfect systems. All systems have flaws and vulnerabilities. And when we think about a change in a system, we tend to evaluate that incrementally. Is it making improvements in some part of the problem that is out there? And, clearly, we ought to worry some about the interactions, but sort of this incremental analysis seems like, certainly in many instances, certainly by far the easiest way to proceed -- and I guess my big-picture question about the methodology is: Is there something fundamentally flawed with that approach to the problem, and if so, how do we fix it? And the second and, I guess, the bigger picture question about US-VISIT and the RFID implementation is that it seems like, to me, the fundamental rationale for this program is we're gathering information that we do not now get, albeit imperfectly, because we have no idea when somebody leaves the country. And so it seems like the really big picture question is, do we need that information? And if so, what are we going to do with it?

MR. NEUMANN: Let me take the big-picture question first, and then the rest will talk about the other one. I think it's a huge problem with the view of incremental change. We tend to design systems. From my own experience, I've seen many systems that were designed for U.S. government, military, whatever, where security was not understood. It was not even specified. And the answer is, "Oh, we'll add it later." I think most of you realize that you can't retrofit something that fundamental into a system unless it was designed that way in the first place.

The second thing is we've come to rely on what's called patch management in mass market, laptop software. Every time you put in a change to a system, you potentially compromise every security concept that you had in the first place. So the incremental notion is wonderful if you have a plan of where you're going in the first place. But if you're just willy-nilly making changes that seem to fix the problems that you've had last week and, in fact, introduce new problems, this is not a convergent process, and we are living in a world in which the marketplace is perfectly willing to put out fundamentally flawed systems and put patches that increase the flaws that are in those systems. Let me stop at that point. But I think you see there are serious risks to the incremental approach unless, you have sound architecture in the first place, unless you use the good software development, and that's not happening.

MS. MULLIGAN: I think there's kind of the pragmatic and the perfect, and you're asking how do we square those two. And it's a difficult question, but I think probably the right answer is that somebody has to be looking at the system, right, and so -- and I mean the system at some larger level. But, you know, you look at the E-passport, and they're like, "Oh, we're not even really changing our own system," right, "This change doesn't really matter." And then you look at the US-VISIT, and one of the things that I think was really excellent about the PIA with US-VISIT is, they not only said, "Well, let's look at the way RFID is going to change," but they looked at the way in which the interaction between all of the various systems of records that undergird that new addition, right, so their concept of the magnification, of the change, and what needed reassessment was quite different than what you saw with the State Department. Right? It was one step broader. And I guess the question is: At what level does our system analysis have to begin? And I actually don't think I would say to the person who's responsible for US-VISIT, "Well, you know what? You're responsible for considering the effects on our global identification system." Right? It's above their pay grade; that's not their job. But somebody's got to do it, and right now, nobody's doing it. Right? Everybody's like, "Well, you go do your little piece" and "You go do your little piece." And at the end, you know, there are two possible scenarios. One is we end up with something which a miserable failure on all accounts, and the other is that we end up with something that works really well and just the unintended consequences are things we just don't really want to live with. So there's got to be both a pragmatic and a perfect, and they have to be pursued in some way on dual tracks. And right now, the pragmatic seems to be getting far more attention.

MR. NEUMANN: "Perfect" is a bad word. Voltaire is a --

MR. TIEN: I don't ask for perfection, but I do ask, I think, for learning. I mean, I think Secure Flight actually in Task II is a good sort of example of incrementalism, sort of being not necessarily very useful. What we have seen in the years since September 11th of incremental work on an identity-based screening system, and what we seem to be driving towards is that we want the system. In order to work, it needs more information, it needs more this, it needs more that. It needs to reach out to commercial data. It needs to do etcetera, etcetera. Is there a point at which someone will say, "Maybe" -- and, you know, EFF always says this in its comments. Maybe the answer is to give up the idea of an ID-checking-based verification system. Maybe that doesn't bring perfect. Maybe accurately screening for weapons and explosives actually significantly or sufficiently controls the danger in the risk of terrorism to airplanes and any incremental or any benefit that you might posit from ID checking actually doesn't -- isn't worth it. But I don't know that anyone ever asks that question. I mean, we ask it all the time. It's almost sort of gotten to be a rhetorical, sort of throw-away because I don't think that anyone ever really considers it. But -- and yes, that's really the big-picture issue there.

MR. NEUMANN: You're saying maybe it's equivalent to bending plastic knives and airplanes.

MR. TIEN: Well, on that note, I will -- The record will reflect that when Ms. Mulligan noted that it was above Mr. Westray's pay grade, he was vigorously nodding his head.

MR. WESTRAY: (Laughter.)

MR. ROSENZWEIG: And in agreement, I want to thank the panelists for coming. We very much appreciate the learning that you've given us. As you could tell, probably if we had twice as long, we'd still be asking questions, but unfortunately we don't. Before we break, I wanted to make an announcement. I was asked. It would be of interest to members of the Committee and members of the public who follow this closely that Secretary Chertoff has today named Maureen Cooney as acting chief privacy officer.

ATTENDEES: (Applause.)

MR. ROSENZWEIG: The Committee will now adjourn to a closed classified session next door for lunch with Mr. Oberman. We will resume here at 2:00 p.m. Thank you all for attending. We'll see you in an hour and a quarter. (Morning session adjourned at 12:48 p.m.)