TRANSCRIPT

PROOF POSITIVE:
NEW DIRECTIONS FOR ID AUTHENTICATION

PANEL 3

APRIL 23, 2007

>>BETSY BRODER

People are having way too good a time here. But if in the meantime, people can take their seats so we can start this third panel. And I'm going to skim over some of the niceties because -- is that me? Or do you hear that? Blackberries?

Because while you may not see her, right on my shoulder is the head of our Office of Public Affairs who is reminding me that we need to leave this space in time for the advance team to come up and set it up for the press conference that will begin at 1:30, and they need to get the room cleared soon before that. So we're going to try to move quickly along here.

But we're really exquisitely positioned because so far this morning we've been talking about strengths and weaknesses of different approaches in a meta-sense, in the large theoretical sense of how we deal with identity. And at this panel we'll speak more specifically about how those challenges have been addressed and dealt with or the challenges that they still present in existing systems that have been implemented or that are being planned to be implemented, from birth certificates to passports to drivers' licenses to private industry authentication issues. And so let's just get right into it. As with all the other panels, it's quite a distinguished group of participants.

Our first speaker is Garland Land who is the executive director of the National Association for Public Health Statistics and Information Systems. He has been at NAPHSIS since 2005, and before that he actually saw it from the frontlines when he was a state registrar for vital records in the state of Missouri.

Our next speaker will be Patty Cogswell. And she is on temporary assignment as the acting associate director for the Screening Coordination Office at the Department of Homeland Security. And her portfolio includes harmonizing policies and investments for identity management and people screening activities.

Our third speaker today is Toby Levin who is, perhaps, her highest credential is that she's formerly of the Federal Trade Commission, and it's always wonderful to have her back. Toby is also with the Department of Homeland Security. She works in the Privacy Office advising the chief privacy officer on internal and external privacy matters and she's very much involved on the privacy issues related to Real ID.

David Temoshok is the Director for Identity Policy and Management for the Office of

Government-wide Policy of the General Services Administration. Now this is a difference between government and the private sector. Would you ever have anyone at your bank with a title that long? But he's going to talk to us this morning about government implementation of HSPD-12, which has to do with the standardization of federal credentials and how that is coming along, and again the challenges that we see in that respect with the whole authentication universe.

And finally, representing the entire private sector, is John Byrne from the Bank of America. He recently joined the Bank of America after spending 22 years with the American Bankers' Association. In 2007 he became Regulatory Relations Executive. Very nice. Elegant. And is responsible for working with federal and state agencies, non-US regulators, and industry organizations on various regulatory and risk issues. We thank all of you for being here today. We have two other participants who we call our discussants. Selden Fritschner is with AAMVA. He's on the front page. Selden, he's the Vice President for Law Enforcement in the American Association for Motor Vehicle Administrators and he, too, is looking closely at the issues related to the implementation of Real ID and general authentication issues. He also probably brings a perspective on the need, in certain contexts, for centralized databases because his background is very much one of law enforcement. In that respect he is an integral member of the team here and our approach on identity management.

Our second discussant is Ari Schwartz. He is the Deputy Director for the Center for Democracy and Technology here in D. C. Very much active in promoting privacy protections in the digital age and expanding access to government information via the Internet. As we heard in our first panel with Simon and Gus, probably the largest issue that we deal with in developing appropriate identity or authentication approaches has to do with privacy. So he will be a key stakeholder and we're looking towards his insights on the issues that have been discussed so far.

So the sequence of our panel is first Garland will speak, then Patty, Toby, and David and John. The final four have PowerPoint presentations to talk about some of the high level issues in their authentication issues, and then we'll have Ari and Selden weigh in and a discussion of all of the issues. Thank you. You may notice that I'm the only one up here that doesn't have an identity. So as people get up, I will take their identity. So Garland, if you could please.

>>GARLAND LAND

I'd like to give you a little bit of a background on the vital statistics in the nation, and some of the changes that are going on. Some of them are automated activities and some are other changes. The state vital statistics for the United States is a state system. It's not a national system. Not a federal system. It's governed by 57 jurisdictions, all the states, the territories and D. C. and New York City. And those are where birth certificates are registered. There are over 6,400 local jurisdictions in addition to those 57 that issue birth certificates. What kind of holds that system together is there are model laws and model regulations that the states have passed that are somewhat similar from one jurisdiction to another, but not exactly the same.

The birth certificate has been labeled as a breeder document because if you can get a birth certificate or have a birth certificate, you can then get a passport, you can get a Social Security

card or you can get a driver's license. And that basically is what establishes, for the most part, identity to some extent in the United States.

The 9/11 commission realized that there are serious problems with the birth certificate system in the United States, and there have been two federal laws now that have passed that are trying to address some of those issues. One is the Intelligence Reform and Terrorism Prevention Act, and those regulations are going to come out in the fall of this year. And those relate directly to state vital statistics operations. And the other is the Real ID Act, and those regulations just came out this last month and there will be speakers talking about those. But they also impact our operations.

There are basically two ways in which birth certificates are used to create false identities. One is the falsifying of the birth certificate itself. The other is to use somebody else's birth certificate for false identity purposes. So let me talk briefly about each one of those, and how those occur. And there are many other ways that I'm not going to talk about, but just to kind of give you an overview.

The first is that some people create a new birth certificate all on their own that looks identical to a state-issued certificate. And if there are not careful adjudication processes going on, they are accepted by the agency as a valid birth certificate. Or some people obtain a valid birth certificate and alter it. Change the name. Change the date of birth in some way. And they're getting very good at this. And so it creates a whole new record by altering a valid record that was issued.

Another way is, in some cases, people don't have a birth certificate. They were born at home or their birth certificate was never registered. This is a very small percentage of the population, but it does exist, particularly for older people. So there is a process that all states have in which they will create a delayed birth certificate in which the person has to provide basic information to establish the facts of birth and then a new delayed birth certificate is created. Well, some people have figured that process out and provide false information to create the delayed birth certificate. So those ways and probably many others are ways in which fraudulent records have been created in the past.

There are also ways in which people obtain someone else's birth certificate and use it for false identity purposes. Probably one of the best known is they'll look in the obituaries, find a person who has just died, particularly an infant that hasn't created an identity yet, and then they will apply for that birth certificate on that infant and then assume that person's identity.

An open record state, we have about a dozen states in which it's perfectly legal for you to go into that state, request anybody's birth certificate, and they will give it to you. And then you have that person's birth certificate and then you can use it for whatever purposes that you want to. Obviously, that's a serious issue. But it does go on in a lot of documented cases of people assuming somebody else's identity through an open record state.

If you go into my former vital records office in Missouri and if you know enough information about me, my mother's maiden name, my date of birth, my name, where I was born

and so forth and fill out the registration form, you can get my birth certificate. And that occurs also sometimes. Where if you just have enough information about somebody else, even if it's a closed record state, they will issue a copy because there's no way for them, particularly through the mail, to identify who you really are.

Birth certificates of course are stolen. There's a known ring between Puerto Rico and New York City in which birth certificates are stolen and sold in New York City. People sell birth certificates, valid birth certificates. They sell their children's birth certificate because they need the money. So they are actually giving away the identity of their own family members.

So as you can see, the problem's complex. It's not a simple issue. If we just do this one little thing that we can solve the problem of identity theft with birth certificates.

With the Intelligence Reform Act, we made several recommendations of how to close some of these loopholes. All I can speak to is what we have recommended. The regulations come out this fall and we'll find out to what extent those regulations are implementing what we had recommended.

One is that we feel that all states should be restricted states. There shouldn't be open records -- they should be closed record states. You should only be able to get your birth certificate for yourself or for your immediate family member.

We think that there needs to be birth-death matching. So if you request a birth certificate, it's noted in the database that this person has died, if they died, and then that birth certificate would not be issued. Or if it is issued, it will be indicated that this person is deceased. That goes on to some extent now, but not totally in all states.

There's a recommendation in terms of security papers. Some states have very good security paper standards, bank note paper. Others have basically plain paper that they issue the birth information on. So I'm sure there will probably be some standards coming out in terms of security paper.

This 6400 issuing locations I talked about earlier, we think that's a vulnerability of the system. The more people who are issuing at a local level makes it much more difficult to assure that there's consistency throughout the United States. So there's a recommendation to have a central database in each state for the issuance at the local level.

The final area that I want to just briefly speak about is our electronic verification of vital events. They're called EVVE. This is a system that was developed several years ago for the passport, or for the Social Security Administration. It has been piloted with the Social Security Administration. It's been piloted with about half a dozen drivers' license bureaus.

Basically the system operates in this manner. You walk into, let's say, Social Security Administration or into a driver's license bureau or any other adjudicating agency, but those are the two that we've worked with up until now, and the individual gives them a birth certificate. They don't accept that birth certificate on face value. They then enter key pieces of information

from that birth certificate—the name, the date of birth, and either the state file number or the date that the record was filed in the state. Those -- three of those four pieces of information are entered into a web-based application. A message is then sent to the state where the person was born. And then there's a 1 to 1 match to see if that person's record is indeed on file. And if all of those pieces of information match up, it is sent back to the adjudicating agency indicating yes, this is a valid birth certificate. If there's any of that information does not come back, it will give them a hint that says check out the date of birth. Maybe you've transcribed it or something's wrong and then they can try -- we don't give new information back to the agency. They just have to see if maybe they made an error or something.

So that's the system that's mentioned in the Real ID Act. That in the future when people get their driver's license, they will have to present a birth certificate. That birth certificate will then have to be validated. We are also working with passport and we're working with the Office of Personnel Management, federal Office of Personnel Management and we're working with Social Security Administration.

About half a dozen states have been implemented with EVVE. With funding, we expect to roll that out to all the states. And then any agency that has an agreement with us, we will allow them to have access.

So whether or not that's a centralized system or decentralized system, I guess you have to debate that. It's not a centralized system in the sense of a database in the sky or in the federal government, but there are these 57 jurisdictions I talked about that have the birth certificates that were recorded in their jurisdiction. And it's tapping in to see if that birth certificate is on file in that particular jurisdiction.

So, in closing, I think there's a lot of barriers to improving the systems out there. These are governed by state laws, and so whenever there are inadequacies, we have to go state by state to effect change at the state level as opposed to one federal law.

There's inertia, of course, in any government enterprise. And that we've always done it that way is a big problem. And so making changes sometimes is difficult because of that.

And then, obviously, there's cost involved in any of these changes. The EVVE system is actually fairly cheap to install in comparison with a lot of other systems. In terms of what AAMVA has projected Real ID is going to cost, EVVE is very inexpensive to implement, but still it does take a little bit of money to implement and it does take money to implement some of the other changes that I talked about.

So those are things that are affecting our states right now that we're trying to work through. Very conscious of the need for change. And very supportive of trying to make changes that are necessary.

>>PATTY COGSWELL

The first thing I want to do is set the framework and standpoint from a DHS perspective.

At the end of the day, we're responsible for screening. We screen individuals in very, very large numbers. And why do we do the screening? Number one, to identify those who pose a threat. Second thing is to find individuals who are ineligible for something they're applying for or, third, frankly, is to find individuals who have violated the terms of that status, privilege, or license that we have provided.

In that context, you see the kind of numbers we are dealing with and, frankly, the different environments from which we conduct the screening opportunities. I am with the screening coordination office and, frankly, we're so new, most people don't even know what we do. This is a quick plug for who we are and why we are there. What are we doing? The first thing is really looking at creating interoperable environments. I really enjoyed some of the factors brought out by the earlier panel and I'll talk about them a bit more as we move into the next slides, but also it's looking at finding ways to take initiatives and move them from the policy perspective in its implementation as directed to the various pieces of legislation to which we are responding.

One of the first things we have done is a credentialing review. The objective is to look across a life cycle of interactions with individuals, but also look across programs. We want to look at opportunities for fewer credentials, not unlike the discussion we had earlier about why is there not every single store still issuing their own Visa card, version of a Visa card, but now there is a Visa card? We want to look at opportunities to say there should be fewer credentials, not one, but fewer, and that they should make sense given the context in which you're interacting.

We also want to look at, frankly, smarter vetting. And look at a way to simplify interactions of individuals with the Department of Homeland Security.

With that, we have looked at creating a series of principles associated with these activities. These principles are really designed around a couple different key pieces. First vetting, associated with like risks and like usage should be the same. We should look at a way to make sure, frankly, that at X level of risk of an encounter you supply the same information under the same type of vetting so that you, frankly, if you're one of those people who is subject to three different DHS programs, you can go through it once. If you are only subject to one DHS program, you only have to go through it once.

We also want to look at ways to verify immigration status determinations by DHS electronically. Frankly, we see a real problem with using a card, a physical piece of information, as a way to communicate amongst DHS. There is too great a possibility, frankly, that someone could try to create a fraudulent identity. We also want to look at verifying that entitlement to a license, privilege, or status using technology, the signer enrollment programs, so that we can more often enroll once and reuse information where appropriate. And the last thing is really to create a good robust opportunity for redress so the individuals can come in, identify the information, and make corrections where they need to.

As one of the examples since I was specifically asked to talk a little bit more about the travel context is the US Visa programs. It is one of the more well known programs out there

using biometrics. And one of the key things I wanted to talk about is the life cycle idea. The life cycle idea means you expect to come in contact with an individual through multiple different ways, multiple different programs, and frankly, multiple different agencies. Pre-entry at this point in our time is really about the Department of State. I forget who said it at the earlier panel, but they were talking about the need to prevent people from re-applying, double dipping.

One of the biggest things that we've seen through the creation of what's called the bio Visa program is we've stopped individuals from shopping locations to get Visas. Individuals who applied in one context who were denied cannot go to another location with a new identity and try to get a Visa in that new identity.

The second one, frankly, is more of that context, making sure that we can still verify an individual across life cycles. So for example, the person we see at that pre-entry stage who gets that Visa, we can at entry say yes, you are the person to whom State Department issued that Visa. This is very important because, frankly, one of the biggest issues we used to have is called Visa washing. Literally they take that piece of paper, scrub off the photo, replace it with other information. We can now say, oh look, in our system, we show that the person to whom this Visa was given is a woman. You're not. The name is completely different. And, gosh, she was 12 and you're 47. We have a problem that we have been able to solve through this identity management context.

We also look at them further for status management. One of the biggest issues we've ran into, frankly, that we're excited about is recurrent vetting. Quite often the paradigm used to be you vetted someone at a point of encounter and only at that point of encounter. What we have found is an individual may have no derogatory information at the time we captured them at the Visa application, may be clear upon admission, but later they come in contact with law enforcement. And now they're wanted by -- pick your favorite state agency. Because we have a path and a mechanism to receive that information, we can then check that new derogatory information against the enrolled population. This means that an individual who now has violated the terms of their admission to the United States, we can identify them and we can then take appropriate law enforcement action.

Next thing I want to talk a little bit about is the Western Hemisphere Travel Initiative. It is a little bit of a different context in that it's focused, again as some of the other panelists have discussed, its requirements coming out of the Intelligence Reform and Terrorism Prevention Act, that looked at how do we set up an environment so that we don't have 8,000 different birth certificates and all the other things coming across the border? How do we look at an environment so it's very easy to identify individuals who are compliant, individuals for whom there are no issues so we can instead focus our time and attention on those who are not compliant? How do we find the threat? How do we find the risk?

The other piece of it, frankly, is a way for us to quickly automate checks. The key here for us is looking at an environment that will facilitate the travel across the border because this country thrives on that kind of economy and transmission between countries.

Some other things I wanted to really focus on here in particular is some of the recent

contexts about the Department of State potential passport card that we've had a recent set of regulations discussing, and the comparable DHS regulations that go along with them, about what documents will be expected for border crossing.

Right now the proposal is for that card to have a machine readable zone, that lovely little thing with all those carets you see at the bottom. And a vicinity RF. Longer range read RF. The key here on the radio frequency is a number. The number doesn't mean anything. It's not a number that can be generated from anything specific. It's truly a random number issued by our system. The key here is really that we are able to take that number and tie it to a record about you so that when you come across the border, there is a place you come to get into the queue to come up to the booth. It reads that card or, frankly, several cards that are in a vehicle and prepositions that information for the customs and border protection officer. They can then see the photo of the person, this is who it was issued to. And also all the information about background checks that have already been run. So that the officer can know right then and there does this person present a threat or is this no record, no issues?

That's kind of how we've been approaching it. In particular I wanted to note two items. Number one, this is the next generation of radio frequencies similar to the Nexus century fast technology that we have been using since 1995 on the border.

The second item is we intend to issue it with a sleeve. This sleeve is intended to block all transmissions off that chip. So if it is out of the sleeve, you can read it. When it's in the sleeve, it is not readable.

The next item I wanted to cover is the E-passport. Also back in that travel context. Again as part of the Intelligence Reform and Terrorism Prevention Act there was a requirement, I'm sorry, this was the Enhanced Border Security Act, there is a requirement that DHS be able to biometrically compare and authenticate travel documents from various, the Visa waiver nations, the 27 different Visa waiver nations.

The way we have approached this in the international community, these standards set by the international civil aviation organization, is through the creation of what's called a proximity radio frequency identification chip. Sometimes also called the 14443 chip for people who are really into this. The way it works is a couple fold.

Number one is that the machine readable zone down at the bottom of the document must be read to unlock the chip. You can't just read the chip off the document. That is how the vast majority of countries are producing the document. That is how the U.S. is producing its document. In addition, the U.S. is doing something beyond that. They also put protective materials into the cover of the book. So that when the book is closed, the chip cannot be read. It has to be opened to be able to be read.

The last thing I wanted to show you is, frankly, just some examples of the various equipment that you can see in use in the border community. So the first one up there on the top left is a standard swipe reader, reading those characters so that you can see kind of how that works. The bottom two are the two biometric capture devices currently in use at our borders for

those for whom we take a photo and a fingerprint. The document in the middle is that E-passport reader. So you can see you have to actually physically open the book, put it hard into the reader, so it can read that MRZ, and unlock the chip. And then the last two over there are the two ten print slap devices that we are currently looking at prototyping and piloting coming up in the relatively near future. The State Department is already in the process of using them, as well.

I think I covered everything. Thank you.

>>TOBY LEVIN

I have about five minutes to convey to you the Real ID, which is an impossible task. So buckle your seat belts and drive warp speed. I hope you'll take time to look at these slides, which will be on the FTC website independently at your convenience.

The Real ID was basically the recommendation of the 9/11 commission to improve identity documents, in particular drivers' licenses. All but one of the 9/11 hijackers had acquired some form of U.S. identification, in some instances had multiple drivers' licenses.

What does it do? It sets a minimum standard for state-issued licenses. It increases the security and integrity of state-issued licenses. Makes, the Department believes, the nation stronger, safer, and better protected against terrorism and identity theft. Protects individual privacy, respects authority and the functions of the state, which traditionally have done licensing, and increases confidence that people are who they say they are.

It creates minimum standards for licenses and ID cards for official purposes and the Act and the implementing proposed regulation defines that as accessing federal facilities, boarding federally regulated commercial aircraft, entering nuclear power plants, and then we have invited comment on any other additional purposes. I should mention that the proposed regulation was published on March the 9th and the comment period closes on May the 8th.

At a minimum, each card must include this list of data elements. And applicants are required to provide a number of documents. This slide indicates those documents that are required to demonstrate citizenship. And in addition to providing those documents, individuals applying for license will have to document name change, establish their date of birth, which can be through one of the prior documents, establish Social Security number if they're eligible for Social Security; if not, evidence of why not? To establish their address of principal residence and establish lawful status in the U.S.

Very importantly, states, then, with this documentation, must verify the data. And of course with training, DMVs are very experienced in trying to assess whether a document is authentic or not authentic. And breeder documents are obviously very difficult in terms of authentication. But through the Real ID, the statute and the implementing regulations call for the data on these documents to be verified with the issuing agency. So I think the best way to demonstrate that is to look at this slide. On the left-hand side, on your left-hand side, demonstrates the state's DMV processes in terms of authenticating individuals. And on the right-hand side, the data verification as it will occur.

There are three key balloons there. I guess the top is the employee clearance. Certain DMV employees will be covered employees who are involved in manufacturing or issuance of these credentials, and will have to undergo a criminal history check. That will be done by the FBI. Then the states will check against four federal agencies the applicant data. And beginning with the Department of Homeland Security, SEVIS -- I always have to look at my notes because I can't remember the acronyms -- the Student and Exchange Visitor Information System, which applies to students, exchange students and visitors, and academics. The Systematic Alien Verification System or SAVE. And then also check against NAPHSIS's EVVE system Garland spoke about earlier. The Department of State's Consolidated Counselor Database, the CCD. And then the PIERS - Passport Information Electronic Records System. And then, finally, the Social Security Administration's S-SOVS system which is the Social Security Online Verification System.

Now, not all these systems are available to all the states. There are pilots with regard to the EVVE system. The Department of State systems are not available electronically to the states so the Department of Homeland Security will be working very hard with the federal agencies to get these systems up and running and available to the DMVs. Many of them are available today through AAMVA and we'll be hearing more from Selden. States can check directly, to single checks against DHS, for example, or SSA, the SSOVS system. But the Department has proposed exploring a federated query to allow the states to do this checking in a much more streamlined fashion.

And then finally, the state to state data exchange, and that is to reflect the fact that, under the Real ID Act, you can only have one Real ID. So that states, when you apply, will want to make sure that you don't hold a Real ID license in another jurisdiction.

And I should stop it for a moment and say that concerns have been raised about whether or not people will be able to fly or enter federal buildings if they don't have a Real ID after the effective date of the regulation. The answer to that is yes, you will be able to enter buildings. You will be able to fly. What it means is that if you were going to present a driver's license for those official purposes, it will have to be a Real ID license. But facilities and airplane carriers, or the TSA agency, when it takes over all those functions in the future, will want to see a Real ID driver's license. But they may also accept a passport. Or you may be asked to go through additional screening in order to travel or enter a building.

Now, to the minimum security features that are to make the card itself more tamper-resistant, I'm unwilling to say tamper-proof because I think that sets the bar too high. Some of these features are currently being used in a lot of states. Some states may currently have almost all of these features.

Now, to the issue near and dear to my heart and to the Department's Privacy Office, are the privacy considerations that are raised by the Real ID. When the proposed regulations were released, we also issued a privacy impact assessment, which is posted on our website and the link is provided at the end of the slide presentation, and it identified the following key privacy issues.

Does the Real ID Act and regulations create a national identity card or database? Well, I think the answer is, it depends. It will depend on the use of the unique identifier and what the nature of it is. Will it be unique to a state or will it be unique across all jurisdictions? What will be the nature of the query of the federal reference databases and the nature of the state to state data exchange?

Secondly, how will personal information required by the act be protected in the state databases from unauthorized access or use?

Third, how will the personal information stored on the machine-readable zone, which is mandated by the act, be protected from unauthorized collection and use? The NPRM proposes a 2D PDF bar code 417 which is currently being used in, I think, about 45 jurisdictions. It does not -- it's not currently encrypted or protected and may be read by 2D bar code readers that are fairly common. And some of you may be aware that there are news reports of the 2D bar codes being scanned at bars, convenience stores, where they're appropriately doing age verification, but possibly also downloading information from the 2D bar code.

So the NPRM seeks comments on how to protect the information and notes the benefit of encryption, but asks -- reasonably asks -- about the feasibility of such a system given the need for law enforcement's quick access to the information on the bar code.

And then, finally, how do the requirements for photograph and address on the ID as well as a DMV employee background check, which includes criminal and financial history, impact on privacy? Importantly the NPRM proposes a comprehensive security plan for DMV facilities. And this is significant because within the elements set out within the NPRM is the requirement that there be information protection and security safeguards. So we've invited comment on what those should consist of and demonstrate implementation of best practices to protect privacy based on fair information principles.

Of significance is the architecture of the data system. We want to build on some of the current operations certainly because of the significant cost involved in implementing Real ID. They've been estimated at anywhere between $11 billion and $23 billion. So there's a sensitivity with regard to the building of the architecture in a cost-effective way for the states. But we want to see that this architecture is built in such a way that it minimizes data collection and centralization to the extent possible and protects the privacy of personal information that's collected and maintained.

We're concerned about how the data systems will be governed. And we want to make sure that there are privacy protections and security safeguards that reflect fair information principles. And this slide simply identifies some ways in which those principles can be implemented in an ID system such as the Real ID. These were not identified in the NPRM, but these are ones that our office applies in all the work that we do.

So the last two slides are the milestones. And I would just bring to your attention that the effective date is May 11, 2008. We don't expect all the states to be able to be in compliance by that date. So the NPRM proposes a five-year phase-in implementation. We hope some states

will be up and running for the 2008 deadline. More to come in full compliance by 2013.

So I look forward to your questions. And there is a link to the NPRM and the privacy impact assessment.

>>BETSY BRODER

Thank you, Toby. Our next speaker for the next five minutes is David Temoshok from the General Services Administration. Thank you so much.

>>DAVID TEMOSHOK

Thank you. I'm going to very quickly go through what the requirements are, as well as some of the background for the federal government identity program which was implemented under presidential directive HSPD-12. HSPD-12 is Homeland Security Presidential Directive 12 signed by the president in August 2004. Now, there are four key control objectives within the presidential directive that identity and vetting of identity information be based on sound criteria. Those are specified in a standard published by the National Institute of Standards and Technology called FIPS 201. That standard, the program called Personal Information Verification Program or PIV and HSPD-12 really can be used synonymously.

The second key point is that the cards are strongly resistant to tampering and counterfeiting. There are extremely secure anti-counterfeiting measures deployed on the cards. These are smart cards with associated credentials. I'll go into a little bit of what that is.

The presidential directive requires that these cards not be used as a flash pass, but be used to validate and authenticate identity electronically. There are multiple use cases for that electronic authentication. And you've heard a lot about centralized and decentralized systems, but the presidential directive requires that the cards be issued by issuers whose reliability have been established and accredited through a reliable process, and I'll talk about how that is being done across government.

Key milestones: the President signed the presidential directive in August 2004. NIST was given six months to establish the standard for the federal government. They met that time frame.

The next key milestone that we had was the identity vetting portion of the standard to be implemented in October 2005. The identity vetting standard requires both controls in the enrollment process, but also background checks of all individuals. Background checks and background investigations. It applies, the presidential directive applies, to all federal employees and contractors outside of the intelligence community.

October 2006 was the next key milestone, which was the initiation of issuing the badges, the cards, for all agencies and departments, to replace whatever badges are currently being used.

Next key milestone on this chart is October 2008, where we will have converted all of the

current employees to that PIV program, the PIV pages. We're not done. But these are just key milestones to get the credentials into the hands of verified individuals.

What this chart is intended to show is that we don't see authentication of identity as just one flavor; but, in fact, depending upon the level of access control that's required and the assurance for authentication, that we support multiple levels of authentication. We see the HSPD-12 PIV card at the very highest level, supporting multi-factor authentication if it's needed. There are other levels of authentication capable within the PIV card.

The card itself supports visual credentials. Well, there's a badge, there's a picture, there's printed information on the card. The card supports the concept of a CHUID. A number associated with each individual that's enrolled into the program that can be shared. Consider it like a credit card number where there are different fields within that number that have different meanings to the account holder.

The card supports PIN-based authentication in order to access information on the chip. It's mandatory that the card and the system support fingerprint template biometric on the card as well as encryption-based asymmetric key credentials which are managed through authentication certificates. There are additional credentials and technologies that may be optionally supported on the card.

Across government, this is really about trust, supporting identity federation where identity management and vetting is supported by multiple agencies in order to trust this card has been properly issued and has been issued to, in fact, a vetted individual. That trust is mandated through the presidential directive. It's mandatory. It's mandated through the standard. As well as interoperable technologies which allow information to be exchanged.

One of the things that we've talked about, centralized or decentralized systems, may not be the key point. If you've got separate issuers with separate databases and you expect to exchange information, you need to be able to do that in a meaningful, interoperable way. One of the things we did was identify 22 different categories of products, with NIST, required for HSPD-12 implementation to test against conformance to the standard, the FIPS 201 standard. We do that in laboratories today and publish an approved products list. We require all agencies to use those products in order to insure that data across systems can, in fact, be interoperably and meaningfully shared.

So where are we today? There's more than a dozen agencies that are implementing, consider them stand alone or separate HSPD-12 systems. There's over 100 agencies that have said they don't have the technology expertise. They don't see the reason to implement a separate HSPD-12 system within their agency. They're looking to share infrastructure, to have an issuer, an agency, provide that service for them.

There are four designated shared service providers across government: Department of Defense uses defenseman power data center. Department of State services eight international agencies that are typically housed by them. Department of Interior provides personnel services for 25 plus agencies. This is a direct corollary to that. My agency, GSA, provides services

available to any other agency in government, 40 plus agencies have signed up to us -- with us. We are testing all of the cards that are being issued by the 16 plus different HSPD-12 systems to make sure that the data on the cards and in the systems, the back end systems, can in fact be shared in a meaningful and interoperable way across government.

Again, trust and interoperability is what HSPD-12 is all about. So that we can have common, trusted access to federal facilities and federal systems for all government entities.

And so the conclusion. In implementing -- in issuing the cards that comply with the standard, in converting all of our current employees to that program in October 2008, this is still just the start of how we manage electronic access and physical access for all personnel to systems on an ongoing basis. So this is the start of where we're going in federal government. It is certainly not the end.

And one of the points on this chart is: Can other entities use the standards, the policies, the systems, the approved products that we have? We say it's a standard for the federal government, but it can be adopted by other entities, as well. And we'll point to the approved products. We'll even test systems to insure that interoperability.

>>JOHN BYRNE

What I'd like to talk about is kind of the practical implications of all these issues on an industry like the financial services industry and give you some sense of how we are very dependent on, obviously, what the government and the private sector are doing regarding data. I'm going to focus entirely on our requirements at account opening, what we look at in terms of our requirements under something that we all know as the U.S. Patriot Act.

Let me say up front that there is some confusion. There has been confusion for years, that what we're talking about is know your customer. Know your customer is a different concept within financial services. Know your customer is what happens once you've been engaged with an institution and we look at transactional activity and other things and make decisions about what sort of due diligence we must do regarding your activity with us.

Customer identification programs are the regulatory obligations that our industry faces under the U.S. Patriot Act. Briefly, what we're required to do at our institution, we open up millions of accounts a year. You can open up accounts in two ways. You can open up accounts online, obviously, or walking into a banking center. Typically when you walk into a banking center, you're going to be giving us a document. When you're doing this online, it's going to be non-document verification. I want to focus more of my brief time on document verification because obviously that's what we're talking about today.

The requirements under the Patriot Act are basic. Basic, but as I found out moving to the bank from a trade association, very difficult from a systems perspective to implement. We're required to obtain four pieces of identification. So, when you open up an account with a financial institution, you have to tell us your name, your address, your date of birth, and if you have one, your Social Security number. We have to obtain that information.

But under the regulations, we have to attempt to verify that information. We don't have to do a 1 for 1 match. So as you heard today, a lot of what we do in terms of authentication is really dependent upon the information that's given to us after it's been processed from the states or the federal government. So that information is required to be obtained. We have to do a risk-based analysis on what we verify.

So, for example, we may decide that if an address doesn't match, that's not as important as the date of birth and whether the Social was validly issued. So banks go through their own decision-making regarding risk assessment. So that's something that's relevant because it's not a 1 for 1 match.

These requirements have been in place only since October 2003. Certainly prior to that you were giving information to financial institutions, but it wasn't under a particular mandate. The key elements, as I've already mentioned, is that we collect the data and we attempt to verify. I've been asked to talk about this because we believe it has a side benefit. We can arguably say that some authentication is done through this process because we've collected the information and tried to authenticate it through the documents that you've given us.

If you're doing this online, we are going to use an outside private sector source, non-documentary verification. If you're going into a banking center, you're going to give us some document. We accept what's required under the Patriot Act, and that's a government-issued identification document with photograph or similar safeguard. That's what the regulations state. That could be a passport. That could be a driver's license. It could certainly be a foreign-issued identification document. It can be, as we've seen in the press, a matricular card if it has a photograph and obviously it's consistent with the regulations.

So the bottom line is we collect these records, we attempt to verify the information, and we have a process at our bank, as do many other banks, to repair deficiencies. If there's not a match, if there's a problem with the documents, we go back and try to repair those problems. If we can't repair those problems within a reasonable period of time, most institutions will close the accounts. So that's sort of the check on authenticating identity. It's not 1 for 1, but obviously it's a help.

In addition, it's for recordkeeping and verification, and we're examined. So we're examined by the federal regulators to see what our programs are. Typically they will go in and assess what our policies say regarding the information we can collect at account opening, what's our verification process and they'll go through and test the processes. We are also being tested by our own internal audit function and some of us have our own self-assessment program. So there's a way to see if the financial institutions are following the letter of the regulation and whether that process exists. The regulators again are a test to our program to see whether, in fact, they are following those requirements.

Jumping up here, one of the positive aspects is we believe this assists in fraud prevention through both the use of the document verification and the use of external sources. So whether it's Dunn and Bradstreet, whether it's Lexis-Nexis, one of those processes we will look at to see

that the information we have is valid as much as the information can be tested through those processes. We think that helps in fraud prevention, although most of what we are doing is to prevent money laundering and terrorist financing in terms of the customer identification program.

Challenges going in the future? Bottom line is it's risk-based. There's not a 1 for 1. So to depend totally on the bank if you're working with us from a third-party perspective, there are going to be some gaps because again we're required to obtain, but we're not required to verify, every piece of information.

We've also heard today the varying level of strength in the documents, in the databases. So we're very much dependent on what the drivers, the motor vehicle groups are doing, what the passport issuance processes are doing, what homeland security is doing. We're depending upon the government in those situations to do the hard work. So again it is what it is. It is only as good as the documents we are relying upon.

Social Security numbers, for example, is not a 1 for 1 match. You can see whether the number was validly issued, whether it's on a death master list. We certainly do some due diligence there. But there's not a 1 for 1. So we're really dependent on the outside sources.

Foreign versus domestic identification documents, when we started the debate several years ago, I think, it could be argued that some drivers' licenses issued by some states were pretty faulty. We've obviously seen from a policy standpoint that's been improved dramatically. But from our perspective, foreign documents versus domestic documents, we can accept both. We obviously have to look to groups like AAMVA and others to work very hard with their organizations to strengthen that documentation, but we have no control over that.

Finally, the general impact on the economy. There has been some debate in this corner and I was asked just briefly to touch on this. Throughout the process of finalizing these regulations, there was some debate whether or not financial institutions should be able to accept foreign documents like the Mexican matricular card. Obviously that was a heated debate. It touched a lot on immigration and on issues unrelated to identity. We have seen the public comment several times when the Treasury Department has asked publicly should that be accepted, and overwhelmingly the public has said that should be an acceptable document. It's currently allowed. We do accept it. If that were to change, however, then obviously our requirements would change.

Bottom line is: we believe that we do a lot of other things to help authenticate information. But from the standpoint of these regulations, we do think it has a benefit of helping the customer know that we have these processes and programs to attempt to verify the data that they've given us.

>>BETSY BRODER

I think we could probably spend the rest of the day just kind of teasing out from each of these applications some of the challenges and problems, but I want to circle back to our first

presentations, the famous Simon and Gus road show. I wrote down lots of things, "we're not gentlemen" was the first thing I have. And something about dogs to the dinner bowl.

But the real point that I want to circle back to is Simon mentioned being at the sharp, jagged, and bloody edge of identity policy. And whether we find ourselves here, kind of teetering on that edge, being given a certain mandate, trying to implement it, but perhaps not being able to step back because of a legislative mandate or being too close to it to understand what these other issues are. I'm also thinking a lot about the concept of usability and putting consumers first, having a consumer-centric model so that it can be applied in a way that works well across the board.

And so with those things in mind, I thought I would like to ask Ari: Well my first question was, what is wrong with this picture? But I think I'm going to rephrase it a little bit. Simon and Gus also talked about consumer acceptance having to do with trust. And who has the information and how it's going to be used. It's one thing to have an identity policy that is housed or owned, if you will, by a government entity that is associated with consumer well-being. People have a different reaction, at least they did in the UK, when the identity policy was going to be housed in the Home Department, which people associated with law enforcement, the government presence. And suddenly the comfort level was much lower. So with these things in mind, I wonder what your feedback is on the various models that we've heard about so far this morning?

>>ARI SCHWARTZ

Well I guess to start with, I'm reminded what Jim Harper said when he first started which is he didn't have anything to criticize yet because there hadn't been that much put out there, but there's been so much on this panel that I sort of wish Jim was here to help me out a bit.

To start with, let me first point out that CDT has done this set of identity privacy principles that we have out on the back table. They are in draft form. We want people's comments on them, but that's sort of the basis for the way that we evaluate these systems today. I think that there are a lot of positives that we heard from here and a lot of negatives on the privacy side.

Garland started off and went through -- let me start with some of the positives. Garland started off, he talked about birth/death matching and securing the documents, the breeder documents, et cetera. Those to me seem like very common-sense, strong beginning points. Obviously, the devil's in the details, to some degree, but those are the types of things that may actually end up helping in privacy issues, cutting down on identity theft and other concerns while having very little impact on privacy and helping the entire system to work better, if we can get them done.

The next one I wanted to comment on was David Temoshok. We have worked pretty closely with David on some of these issues. He's gone along. And I wanted to point to people and make sure that they saw the risk assurance levels that they put together and made comments on that are really the best thing that we've seen out there in terms of breaking down different

kinds of uses for a document like an employee card. A lot of thought went into that and it's something that shows that the stronger the authentication is doesn't mean you want to use it for everything, for all purposes. You need different kinds of authentication for different purposes and you need different kinds of -- identity doesn't even come into play until you come into some of the higher levels of the risk level.

Places where we have more concern, I'll start with the one that I think is probably the most concerning, at least in terms of implementation, and that's the pass card. Patty went through some of the issues in a positive light there. I think the implementation of it, I mean as far as something that people may use out there, it's a useful -- potentially useful tool for people out there, but the current implementation of it borders on reckless. And think about this. It has nothing to do with security. The pass card has nothing to do with security. If it had to do with security, they would have people using the E-passport. It has to do with convenience and cost. Those are two legitimate concerns to get down to, but we shouldn't sacrifice security and we shouldn't sacrifice privacy for that particular convenience.

And let me give some examples of this. You don't have to speak to me about the potential privacy concerns and security concerns of using the EPC global, what the State Department and DHS are calling vicinity read ID, in an identity card. Speak to the people that created the standard at MIT, who have said that you should not be using this form of RFID in identity documents. There's never been a test of the two systems that Patty mentioned -- nexus and sentry -- an independent verification test. Yet we're using it on a broad scale.

Patty said that this was a randomly generated number. Well of course it's randomly generated before you get it. I mean any government ID number doesn't mean anything until it's put into the system. But once you have it and the government has issued it to you, it becomes an identifier. Right? They are creating new identifying numbers for people that get the pass card.

The only positive thing that could possibly be said about the privacy implications for the pass card is that it's a voluntary system. And we have to do a good job if they're really going to implement it this way. We have to do a good job in explaining to people what the real risks are for them out there of having this card, the security risks. I think that's especially true for people that are being stalked or have threats of being stalked et cetera, who then can be tracked by this number in the future that can be read from a long distance away by virtually any reader.

Remember, this chip was created for use for tracking items in the warehouses. It is not created for tracking people. And now we're using it in this way that has potentially a very big risk. I know I don't have much time. So let me just quickly get to Real ID, as well.

I think Toby laid out some strong things that they're doing to try and really recommend privacy protections in Real ID. There are some basic problems with it, though. And most them come down to the law and the way DHS has read the law. Toby had that slide, which actually is the best slide I've seen in terms of laying out all the different pieces that make up Real ID -- at the bottom it had a privacy protection across-the-board at the bottom there. But when you read the DHS NPRM on Real ID, it specifically says we don't have the ability to really protect privacy because Congress did not give it to us. I disagree with that premise because it assumes

that security and privacy are separated in this space which a lot of times we spend time trying to separate out privacy and security. But in this space, when you're talking about identity they actually go hand-in-hand a lot. We think that DHS can do more to protect privacy in the name of protecting security. If you have identity theft, it's both a privacy and security threat and a threat for the entire system in this case.

But we also think that there are other ways that you can build in privacy protections. There was a discussion earlier, Tom Oscherwitz asked a good question about creating decentralized systems from government and how you go about doing that. This seems like a natural fit. Here we have AAMVA sitting right next to me. You have 56 jurisdictions that have all this information, that are collecting all this information, that are storing all this information in a decentralized way. Why not create as decentralized a model, a database, for accessing that as possible rather than creating a centralized system where you have both the threats of a centralized model and the threats of a decentralized model because the information is stored in the states as well. We think there are ways to go about doing that and we would hope that DHS would be creative in those ways and if it takes -- if that means upgrading the states and needing more money to upgrade the states, the smaller states and the systems that they have, we may want to roll this out in a slower time frame than trying to rush and trying to do all of this at the same time.

There is benefit from some of the other pieces of Real ID, such as strengthening the card itself, strengthening the issuance process. Someone said on an earlier panel that CDT did a report on weaknesses at DMVs. We found that we think the weakest link in the chain is the ability to bribe the DMVs themselves, the people that work at the DMVs. And background checks only get you so far as that goes. The people that are going to be working at DMVs probably haven't had the history of being in a position to be bribed, to create licenses or create some kind of identity, in the past, so it's a new kind of threat for them.

The physical security of the DMVs as well is only slightly addressed in the NPRM. We think that those areas are probably the place to start and let's work down the road at getting at some of these bigger issues as we build the states up to the same level, rather than going to the lowest common denominator at the states and providing the ability for the Feds to access it.

One other point that's worth mentioning is they had the drawing of the privacy protection across-the-board. There is a question if you do have a centralized -- any centralized set of information -- where that's held and what protections come under it. If it's at DHS, what protections stop it from being shared with other people within DHS? If it's held in AAMVA, the way some people have discussed, where's the privacy act protections that you have? There's actually no protections for the information being held by a third-party. You don't even get the state DMV protections at that point.

There are drivers' license protections at that point. So there's a number of potential threats in how this architecture actually shapes up and how we end up implementing it.

>>BETSY BRODER

Thank you. Selden, if the Social Security number has always been thought of as the de facto identifier, and we're only now realizing what a mistake that was, maybe the drivers' license has been considered the de facto identification card. And here you have all of the support of the federal government behind the states to insure its greater authenticity. What's the problem, if any, with Real ID from your perspective?

>>SELDEN FRITSCHNER

So many notes and so little time.

>>BETSY BRODER

Besides money.

>>SELDEN FRITSCHNER

I rest my case. I need to make a couple of clarifications. And I sit here listening to the same kinds of discussions we've heard since 9/11. First of all, let's think about the original role of the driver's license. The driver's license was created to prove you had the ability to drive.

AAMVA represents 56 jurisdictions throughout the United States plus several in Canada. Think about the implications of that to the governor. The motor vehicle association, the DMV, is the number one customer base for any governor in this country. And the reason that I felt like I should wear a flak vest up here when I sat through this two-day conference is because it all comes down to internal fraud or long lines or inefficiencies that are perceived. And yet there are other threats to the data that we hear about that I don't see represented. So I'm not trying to be defensive. I am trying to paint the perspective to get to Betsy's question.

We've seen in recent weeks identity that's been stolen from retailers. We know of identity that's been threatened from government agencies. We know of identity that's been threatened as a result of stolen or mislaid data from universities.

So let's keep all of this in perspective. There is always a potential for internal fraud, no matter what happens, if you have access to private data.

Secondly, AAMVA is all for -- in fact our primary concern with all this is protecting the privacy of the individual. Some of that is mandated by the Drivers Privacy Protection Act that's been there for years.

AAMVA is all for most of the issues that we all as citizens have concerns about as a result of the statement that said all but one of the people who have gone on airplanes had fake DLs. Well, in fact, they weren't fake. They were real. And some of those people had multiple drivers' licenses in their pocket. We recognized this long, long, long before 9/11. But it didn't grab legs until 9/11.

So part of what our issue is trying to do is to come up with a mandate by the federal

government -- and I will finish this without going on because, like I say, I have pages of notes -- and saying when we're told we have support by the federal government, somebody else, not me, made the statement $11 to $23 billion to implement the Real ID that will fulfill all the requirements of what's on these different slides.

And when you talk about centralization versus decentralization, there are 56 or 57 U.S. jurisdictions, and they're all doing it differently. And they're all mandated by their governor. And you've been reading the same quotes in the newspaper that I have. A number of states that are just defying the federal government and saying we're not going to do Real ID.

The Real ID Act doesn't require that every state have a Real ID. It only says you need a Real ID compliant document to get on an airplane. One state has said, you know what, it's cheaper for me to give everybody in my state a passport than it is to reconvert all of my internal systems.

I will say this. Let's think about the process. I didn't come for the first 20 minutes this morning but I did hear the second panel. And this is the picture that is in my mind. You want a secure document. In my own mind -- and I work for an association that represents the people who issue the driver's license -- in my own mind, I think of the most secure document as the passport. The problem with that is: What's it take to get a passport? A birth certificate and a driver's license. Now, when you go get a driver's license, you have to go through the similar kinds of identification processes. So when you go to get a driver's license, what are they asking for? A birth certificate and a passport. I mean, as my son said, we got us a serious situation here.

And to the point about the birth certificates, when you're asking employees to verify all of these breeder documents, by the way, we don't talk to each other. All the federal systems that are there -- there are 14,000 different birth certificates out there, forget the 6500 people that are issuing it.

My only, if I had one slide to that point, and I go around with the Federal Trade Commission and other agencies that train local law enforcement on this, I have a picture, a slide show of five different birth certificates in my family. Five different, legitimate, legal birth certificates. There are only three people in my family. And I don't mean to be trite. I'm just saying let's deal with the issue.

Centralization versus decentralization. There are goods and bads for all of that. But $11 to $23 billion is a huge issue. And 57 jurisdictions trying to do what's right in protecting your data and then going right to the heart of what the DMV is there for, which is highway safety. We were invented for highway safety. We were not invented for identification verification or establishment.

So if somebody else wants to create whatever card that Betsy is calling this, that's fine. The DMVs will take that card and verify your identity with it.

But let's go back to my first question. When was the last time you pulled out your

driver's license for the purpose for which it was intended?

>>BETSY BRODER

Let me ask the panel, everyone on the panel, following up on an earlier thought, very few of us have really talked about Social Security numbers and the role that they'll play in any of your current systems. So if you could give a sense, maybe John, Social Security number, is it important in the process that the bank follows under section 326? Where does it come into play? And should we abandon completely reliance on Social Security numbers as part of the identity process?

>>JOHN BYRNE

Well as I said, you can't do a 1 for 1 for socials. Because the only thing we can do is see if they're validly issued or if they're on a death list. So in terms of their overall value, we obviously have internal identifiers. We rely again on a lot of these other documents. I personally think the social has outlived – again they were also not created for identification purposes – but for benefits as you know. So from our perspective we need additional information to authenticate. Because there are gaps. There are clear gaps. You can't use the social as your primary.

>>BETSY BRODER

Patty?

>>PATTY COGSWELL

For purposes of what I talked about in the travel context, there is extremely limited to no use of Social Security numbers. However, one place that DHS does interact extensively with Social Security numbers, frankly, is the requirement to verify non-citizen's eligibility to work in the United States. And actually that would be the purpose for why Social Security numbers were created. So I think we're actually in pretty good shape there.

>>BETSY BRODER

Is anyone going to stand up for the Social Security number?

>>GARLAND LAND

If I could just talk about, it may not be well known about how Social Security numbers are generated now. When a child is born, the mother has the right to indicate if she wants to have a Social Security number issued for her child. If she does, then that's marked in the creation of the birth certificate and an electronic exchange is then submitted from the health department that receives the birth certificate to the Social Security Administration who then issues the Social Security card back to the child. So there's an electronic transmission system. It's voluntary. She does not have to request the Social Security card. But that's the way

probably 98 percent of Social Security cards are issued today.

>>BETSY BRODER

I have a question for Ari and Toby. And it's reflecting back on the 5 D's, the principles that Simon articulated in developing an identity policy. And I think I have four of those so maybe that's good enough. An adequate discourse. That there is a decision process. That there is a design process that links back both to the decision-making and the discourse. And then there's the issue of delivery. Does it work? I guess that's the fifth. Delivery. Does it work? Is it acceptable? And throughout this whole process, we're re-examining those issues to make certain that this is a system that works both practically and it has buy-in from consumers.

So let's look at this in the context of -- and Selden, also -- of Real ID and measure the development of Real ID against these principles. I'm not going to ask you to grade it, but where you think the process has been very strong and where there might still be some learning to do.

>>TOBY LEVIN

Let me start by saying that the DHS did not choose to let Congress pass the Real ID Act. I wish we had had this workshop for the Congress prior to their issuing Real ID. So we're dealing with just the harsh reality of legislative requirements.

I do think that we have engaged in a great deal of dialogue with the states, with state representatives, and with AAMVA, who is absolutely central to the implementation of the Real ID. Whether we've done the other ones, I'd say the report card is incomplete to a great degree. But I think we were dealt the cards and we're dealing with them.

>>ARI SCHWARTZ

It's actually a great question in terms of Real ID. Toby said that the 9/11 Commission called for Real ID, but in reality they called for driver's license reform. The Intelligence Reform bill actually addressed driver's license reform in a way that we were supportive of.

First of all, it was directly introduced in both bodies, the House and the Senate. It had debates. It had in it a negotiated rulemaking that had all the parties participating in deliberation beginning at that point. We thought that was headed in the right direction. In its wisdom, Congress, and our understanding is it was pushed by the White House as well. So I do blame parts of the administration; I'm not letting the administration off scott-free, as Toby seemed to there.

But I would say that that bill, the Real ID bill, was never introduced in the Senate as a stand-alone measure because its supporters knew that it was going to lose as a stand-alone measure. It was attached to the war spending bill, the Iraq war spending bill. So senators had to decide whether they were going to vote for the soldiers or they were going to vote to repeal the driver's license reform that existed before that had the deliberative process in it. Instead the whole thing was shipped over.

Every time the word privacy was used was taken out of the document, out of the statute, and it was shipped to DHS rather than Department of Transportation. So this deliberative process that we had in place that we thought was going in the right path was usurped by a non-deliberative process that we think is headed in the wrong direction right now. And I think if you look through Simon's -- if you checked off Simon's list you would see exactly why that is. It shouldn't be a surprise then that states are rejecting it the way Selden suggested.

>>TOBY LEVIN

But I do think that the privacy concern has been registered even though the word privacy does not appear in the Act itself. There are requirements now in the NPRM which can be augmented in the final rule. And I think there is a sensitivity to the privacy issue. Notwithstanding the fact that privacy was not at all addressed in the Act itself.

>>BETSY BRODER

I have one very short question. And whoever wants to weigh in on this. We've been talking about the value of interoperability in terms of identity and authentication, and actually I don't know what word to use anymore. All these comfortable words. Now something else.

But there is also an issue of identity creep or use creep, perhaps. And I wanted to know if any of you have thoughts about credentials being used for purposes that go beyond the original purpose of their program. Again, another issue that was raised this morning about, I give my consent for you to use this for a certain purpose, but then it's just so very tempting to expand that to some other purpose. Any thoughts?

>>ARI SCHWARTZ

Well, I think Selden addressed it best in his conclusion about the driver's license. But the one thing that we are concerned about in the Real ID proposal is the lack of limitations for federal uses of the data that's then held either centrally or by the states, both sets of data. And potential transactional data for the use, with the use of that information. We think that it should be limited, because of the mission creep concerns and because of further use concerns, it should be limited to access to DMVs and DMV employees for the purposes of that person's -- for administration of that person's license and by law enforcement for those same reasons.

Beyond that, we think that you're putting the data itself at risk by giving more people access to it.

>>BETSY BRODER

Okay. I'd like you all to thank me -- I'd like you to join me in thanking the panel. (Applause.) It's been a really fabulous morning. I think each panel is building on the other one. I'm going to ask you all now to be back at 2:15 when we resume. Some of you have asked if you will be able to get a copy of the Identity Theft Task Force report when you get back. Yes,

we’ll have copies for everyone. Thank you all. And see you at 2:15.