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

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

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 inel

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

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,1rp-ws th re

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

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.

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.

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

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

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

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

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 implem

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

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

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