AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 107–506

A LICENSE TO BREAK THE LAW? PROTECTING THE INTEGRITY OF DRIVER'S LICENSES

HEARING

BEFORE THE

OVERSIGHT OF GOVERNMENT MANAGEMENT, RESTRUCTURING, AND THE DISTRICT OF COLUMBIA SUBCOMMITTEE

OF THE

COMMITTEE ON GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

APRIL 16, 2002

Printed for the use of the Committee on Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE
80–295 PDF WASHINGTON : 2002

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan	FRED THOMPSON, Tennessee
DANIEL K. AKAKA, Hawaii	TED STEVENS, Alaska
RICHARD J. DURBIN, Illinois	SUSAN M. COLLINS, Maine
ROBERT G. TORRICELLI, New Jersey	GEORGE V. VOINOVICH, Ohio
MAX CLELAND, Georgia	PETE V. DOMENICI, New Mexico
THOMAS R. CARPER, Delaware	THAD COCHRAN, Mississippi
JEAN CARNAHAN, Missouri	ROBERT F. BENNETT, Utah
MARK DAYTON, Minnesota	JIM BUNNING, Kentucky

JOYCE A. RECHTSCHAFFEN, *Staff Director and Counsel*
HANNAH S. SISTARE, *Minority Staff Director and Counsel*
DARLA D. CASSELL, *Chief Clerk*

OVERSIGHT OF GOVERNMENT MANAGEMENT, RESTRUCTURING, AND THE DISTRICT OF COLUMBIA SUBCOMMITTEE

RICHARD J. DURBIN, Illinois, *Chairman*

DANIEL K. AKAKA, Hawaii	GEORGE V. VOINOVICH, Ohio
ROBERT G. TORRICELLI, New Jersey	TED STEVENS, Alaska
THOMAS R. CARPER, Delaware	SUSAN M. COLLINS, Maine
JEAN CARNAHAN, Missouri	PETE V. DOMENICI, New Mexico
MARK DAYTON, Minnesota	THAD COCHRAN, Mississippi

MARIANNE CLIFFORD UPTON, *Staff Director and Chief Counsel*
MARK L. KEAM, *Counsel, Senator Durbin*
ANDREW RICHARDSON, *Minority Staff Director*
MASON C. ALINGER, *Minority Professional Staff Member*
JULIE L. VINCENT, *Chief Clerk*

CONTENTS

Page

Opening statement:
Senator Durbin 1

WITNESSES

TUESDAY, APRIL 16, 2002

Theodore W. Wren, Victim of Idnetity Theft 4
Mary Ann Viverette, Chief of Police, Gaithersburg, Maryland, on behalf of the International Association of Chiefs of Police 7
richard J. Varn, Chief Information Officer, State of Iowa, on behalf of the National Governors Associaiton 9
Hon. Barbara P. Allen, State Senator, Eighth District, State of Kansas 11
Betty L. Serian, Deputy Secretary for Safety Administration, Pennsylvania Department of Transportation, on behalf of the American Association of Motor Vehicle Administrators 13
Barry J. Goleman, Vice President, Public Sector, American Management Systems, Inc. 15
J. Bradley Jansen, Deputy Director, Center for Technology Policy, Free Congress Foundation 17

ALPHABETICAL LIST OF WITNESSES

Allen, Hon. Barbara P.:
Testimony 11
Prepared statement with an attachment 53
Goleman, Barry J.:
Testimony 15
Prepared statement with an attachment 66
Jansen, J. Bradley:
Testimony 17
Prepared statement 80
Serian, Betty L.:
Testimony 13
Prepared statement 58
Varn, Richard J.:
Testimony 9
Prepared statement with attachments 35
Viverette, Mary Ann:
Testimony 7
Prepared statement 29
Wren, Theodore, W.:
Testimony 4
Prepared statement 27

APPENDIX

Chart submitted by Senator Durbin entitled "Forged Documents (Identity Cards, Record Books, Passports)" with attached photos 85
Chart submitted by AAMVA entitled "77% of Americans favor Congressional legislation to modify the licensing process and ID security" 95
Food Marketing Institute, prepared statement 96
Raul Yzaguirre, President and CEO, National Council of La Raza, prepared statement 98
Michael J. Eastman, Director, Government Relations, LPA, Inc., prepared statement 112

Page

Letter submitted by Mr. Jansen from Marc Rotenberg, Executive Director and Mihir Kshirsagar, IPIOP Fellow, epic.org, electronic privacy information center, with attachments 124
Article entitled "IDs—Not That Easy, Questions About Nationwide Identity Systems," Stephen T. Kent and Lynette I. Millett, Editors, National Academy Press 151

A LICENSE TO BREAK THE LAW? PROTECTING THE INTEGRITY OF DRIVER'S LICENSES

TUESDAY, APRIL 16, 2002

U.S. SENATE,
OVERSIGHT OF GOVERNMENT MANAGEMENT, RESTRUCTURING,
AND THE DISTRICT OF COLUMBIA SUBCOMMITTEE,
OF THE COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:03 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Richard J. Durbin, Chairman of the Subcommittee, presiding.

Present: Senator Durbin.

OPENING STATEMENT OF SENATOR DURBIN

Senator DURBIN. Good morning. This hearing will come to order. Thank you all for being here. Today, the Senate Subcommittee on Oversight of Government Management holds a hearing entitled, "A License to Break the Law? Protecting the Integrity of Driver's Licenses and State IDs."

On August 1, 2001, two men named Hani Hanjour and Khalid Al-Mihdhar drove a van from New Jersey to the Virginia Department of Motor Vehicles office located across the Potomac River just a few miles from where we are sitting this morning. In the parking lot of that DMV, they asked around until they found someone willing to lie and to vouch for their Virginia residency. They met Luis Martinez-Flores and Herbert Villalobos, who, for a price, were willing to help. Hanjour and Al-Mihdhar paid these strangers $50 each and received notarized forms which claimed that the two transients were, in fact, Virginia residents.

Using these fake documents, Hanjour and Al-Mihdhar walked into the DMV, stood in line, like all of us would, had their photos taken, and walked out with authentic State-issued Virginia photo ID cards. The next day, on August 2, 2001, Hanjour and Al-Mihdhar returned to the same Arlington DMV office with two friends, Salem Al-Hazmi and Majed Moqed. Hanjour and Al-Mihdhar helped Al-Hazmi and Moqed obtain Virginia ID cards of their own by vouching that they lived together in the State of Virginia. After all, why should the clerk behind the DMV counter have any doubts? Hanjour and Al-Mihdhar produced their Virginia IDs to prove their in-State residence.

On the same day, Abdul Al-Omari and Ahmed Al-Ghamdi, who were renting a room at a Maryland motel, contacted Kenys Galicia,

a Virginia legal secretary and notary public, through a referral from Luis Martinez-Flores, the same person who was hanging around the Arlington DMV the day before. Al Omari and Al-Ghamdi paid Galicia to have her prepare false notarized affidavits stating that the two men lived in Virginia. Using these fake documents, the two went to a Virginia motor vehicles office and received State-issued ID cards.

On the morning of September 11, 2001, Al-Mihdhar, Hanjour, Al-Hazmi, and Moqed boarded American Airlines Flight 77 from Washington Dulles Airport headed for Los Angeles. They all used their Virginia ID cards to board the plane. The same morning, Al-Omari used his Virginia ID card to board American Airlines Flight 11 in Boston, bound for Los Angeles. At the same airport, Al-Ghamdi used his ID card to board United Airlines Flight 175, also bound for Los Angeles.

We all know what happened to those three flights and another, United Airlines Flight 93, that never made it to their intended destinations that day. Instead, the commercial jets tragically became weapons of mass destruction at the hands of these terrorists. These terrorists bought their way into our shaky, unreliable, and dangerous system of government-issued identification. With these phoney cards, doors opened across America, including the doors of these doomed aircraft.

Since September 11, our Nation has been struggling to understand how such heinous crimes could have occurred here in America. As we reflect upon the events of the past few months, we have come to realize that our system of democracy which allows all of us to enjoy our freedom is vulnerable to abuse by those who seek to destroy that freedom.

The terrorists mentioned above, along with their co-conspirators, knew exactly how to take advantage of our open and free society. In addition to Virginia, these terrorists targeted Florida, a State that at the time did not require any proof of residency from anyone. In fact, any tourist could walk into a motor vehicle office, fill out a form on his own, and receive a Florida license or ID card at that time. At least 13 of the 19 terrorists held driver's licenses or ID cards from Florida. A few of the 19 held licenses or cards from more than one State, including from California, Arizona, and Maryland, while only one did not appear to hold any American ID.

Some received duplicate cards from the same State within months of September. These foreign terrorists knew that a key to their devious plans was to come to America and blend in with everybody else until they were ready to take on their murderous mission, and one way they blended in with the rest of America was to obtain a driver's license or a State-issued ID card that helped them present a cover of legitimacy.

They knew that the driver's license is the most widely-used form of personal identification. Across America, law enforcement agencies, retailers, financial institutions, airlines, and employers acknowledge the presentation of a person's driver's license as an acceptable and reliable method of verifying a person's identity.

The driver's license is also a key that opens many doors. Anyone who can produce a valid driver's license can access just about anything. It can get you access to a motel room, membership in a gym,

airline tickets, flight lessons, and even the purchase of weapons, all without anyone ever questioning you about who you really are. If you can produce a driver's license, we assume you are legal, you are legitimate, you are for real.

The use of fake IDs is one of the oldest tricks in the book for criminals. It is also one of the oldest traditions of adolescence and a rite of passage for teenagers, to casually use a borrowed or tampered ID to buy alcohol or tobacco products or just to get into a nightclub. But after September 11, use of fake IDs is no longer just a teenage trick or merely about drunk drivers, as serious as that is, trying to hide their bad driving records using multiple licenses. It is about our national security.

I want to show you a page from the al Qaeda terrorist manual. I am sure you cannot read it from there, but this was found in Manchester, England. Police officials during the search of an al Qaeda member's home found this particular document and Attorney General Ashcroft presented it to our Senate Judiciary Committee last year. It is obvious that the September 11 terrorists were well trained by al Qaeda. They followed the instructions flawlessly. Here is an example of how successful they were.

Each obtained the form of a photo ID, but it is not only foreign terrorists who use fake IDs or IDs obtained through fraudulent means. Seven years ago this week, Timothy McVeigh used a fake ID to rent the Ryder truck that he drove into Oklahoma City. As part of his plot to blow up the Federal Building, McVeigh picked up a fake driver's license in the name of "Robert King." The card even listed a false birthday of April 19 as some cruel inside joke. That is the day that McVeigh executed his terrorist attack against fellow Americans, which was planned to fall exactly 2 years after the Waco incident of April 19, 1993.

Another example, fugitive James Charles Kopp was arrested in France in March of last year after evading our law enforcement officials for almost 3 years. Kopp was accused of the October 1998 murder of abortion clinic doctor Barnett Slepian, who was shot and killed as he stood in the kitchen of his home in Amherst, New York. With help from other antiabortion activists, Kopp used a variety of fake driver's licenses and passports, changed aliases frequently, and moved in and out of the country.

So as we look to defending America, it is critical that we carefully examine how our States issue driver's licenses and ID cards today and determine if it makes sense for every State to continue to maintain its own unique policy and procedures for the issuance process. For example, some States independently verify the breeder documents, such as birth certificates and passports provided by applicants, while others accept them at face value. Some States ask the applicants' Social Security numbers, others do not. Some States ask for proof of legal status in the country, others do not. Some States take fingerprints of the applicants, others do not.

We also need to examine how secure the cards are themselves. For example, each of the 50 U.S. States and the District of Columbia issues driver's licenses and ID cards that vary widely in the level of security and resistance to tampering, from States that incorporate high-tech biometric identifiers to States that do not even require a photo on their cards.

I recognize many States since September 11 are taking proactive, sensible steps to tighten their DMV systems, but I believe we need a nationwide effort to coordinate those activities.

To help us understand the extent of the weaknesses and loopholes that exist in our driver's license issuance process and the usage of cards today, this Subcommittee has invited seven individuals to discuss these problems and to offer solutions. I am pleased to introduce the following witnesses and look forward to their testimony.

I would like to welcome and introduce today's panel, Ted Wern, an attorney with Kirkland and Ellis in Chicago, thank you for being here; Mary Ann Viverette, Chief of Police of Gaithersburg, Maryland, on behalf of the International Association of Chiefs of Police; Richard Varn, Chief Information Officer for the State of Iowa, who is here on behalf of the National Governors Association; the Hon. Barbara Allen, State Senator representing the Eighth District of Kansas; Betty Serian, Deputy Secretary for Safety Administration of the Pennsylvania Department of Transportation, here on behalf of the American Association of Motor Vehicle Administrators, who have been extremely helpful in putting together this hearing; Barry Goleman, Vice President of AMS State and Local Solutions; and Bradley Jansen, Deputy Director of the Center for Technology Policy at the Free Congress Foundation.

Thank you all for coming. We are looking forward to your testimony. It is customary in this Subcommittee to swear in all witnesses, so if you would please rise and raise your right hand.

Do you swear the testimony you are about to give is the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. WERN. I do.

Chief Viverette. I do.

Mr. VARN. I do.

Ms. ALLEN. I do.

Ms. SERIAN. I do.

Mr. GOLEMAN. I do.

Mr. JANSEN. I do.

Senator DURBIN. Let the record reflect that the witnesses answered in the affirmative and will not be asked to leave. [Laughter.]

That was a joke. I would ask that you limit your oral statements to about 5 minutes. I know that is tough because this is a complicated issue. I will remind you, your entire statement will be entered into the record.

Mr. Wern, would you like to begin?

TESTIMONY OF THEODORE W. WERN,[1] VICTIM OF IDENTITY THEFT

Mr. WERN. Thank you. First, I would like to thank you all for the opportunity of coming here and just let you know how truly honored I am to be a part of this process in any way.

My name is Ted Wern. I am an attorney in Chicago, Illinois, and 4 years ago, beginning in the spring of 1998, a person in Columbus, Ohio, stole some of my mail, and in that mail were documents con-

[1] The prepared statement of Mr. Wern appears in the Appendix on page 27.

taining three vital pieces of information, my name, my Social Security number, and my date of birth. Using that information as well as a fake identification card, that person departed on a crime and spending spree that was unimaginable to me at the time, and I still cannot quite put it into perspective.

There are two categories of crimes that he committed. First, financial crimes. He incurred up to $50,000 in bad debt that I knew about. He had telephone accounts, cable bills, and utility accounts. He was able to board airline flights using tickets issued in my name, of course, purchased with credit cards issued in my name. He was able to rent a U-Haul truck. He was able to rent vehicles. He was able to enjoy all of the financial freedoms that we all take for granted.

The second category of crimes were a bit more bold and these involved traffic violations. This man would be stopped by police—he apparently was not a very good driver. He was stopped by police on four separate occasions and he told the police that he was me, that he forgot his driver's license, and on those four occasions, somehow, the violations went onto my driving record. All along, I had no idea this was happening and these arrest warrants were issued in my name and all along I am just driving around in Ohio thinking that there are not any problems.

One of those occasions was actually a DUI, and under the same circumstances, he was able to convince the officers, by giving all of this information that he had memorized so well and claiming that he has lost his driver's license. In those situations, we think that there was not an actual identity card presented, but it is hard to really know.

The end result was that warrants were issued in my name. I was forced to go to court and appear as Ted Wern under these traffic violations and convince numerous judges that these were not committed by me. Those were the difficulties in remedying the traffic violations, but to be honest, what took more time and much more expense was to remedy each one of the credit accounts that this person created.

For every credit card, and there were many, probably into the twenties, every credit card and every account, there was a half-hour of telephone conversations, numerous letters, notarizing of documents. There is a very elaborate process that one has to go through to clear these from your name, and the most difficult aspect is that you get better at clearing these from your name after you keep doing it. But the better you get and the quicker you clear your record, the more easy it is for him to get more credit because you have now cleared your record, your name is clear, and he can just spend more freely.

The same applies for the traffic violations. Once I cleared the warrants, I had a clear record, so when he used my information to a police officer, he did not get arrested for an outstanding warrant in my name.

With all that said, despite those problems, the financial effects, the inconveniences, the emotional effects of knowing that there is someone out there living a much richer lifestyle than you are living now on your name and on your credit. Aside from all that, I really do consider myself one of the more fortunate victims.

For example, I am an attorney. It is my job to write forceful letters, to navigate corporate bureaucracies and to follow up with people and it was much easier for me to do that. It came natural to me. But there are quite a few people out there who do not have those resources. In fact, I volunteer for an organization out of San Diego, the Identity Theft Resource Center. I help victims in Illinois deal with these problems and I get a couple of E-mails a week from people—bright, educated people who just have no idea how to start and complete the process.

Yesterday, in an attempt to be a little more presentable for this hearing, I decided to get a haircut and the hairdresser happened to be a woman from El Salvador who just 3 months after she came to this country had her identity stolen. At the time, her English was not very good and it took years for her to clear her record.

So despite my problems and the heartache it caused, I was certainly one of the more fortunate victims, especially given that my perpetrator was caught. He is now in jail. He is off the streets. Many people are not that fortunate. Most perpetrators get to stay out there for a while because, as you will hear today, it is a pretty difficult crime to catch. It happens sometimes not even on paper.

So with all of that said, what I would like to emphasize here is that this is an extremely difficult situation to remedy after it has happened to you. It has taken years for me. I would like to say that government and that law enforcement are able to correct these problems really easily, but the reality is, once it is committed, it is your burden as a victim to clear these things up. You cannot ask a police officer or a lawyer to go in and convince creditors that you are who you say you are. That is something, as we all know when we make telephone calls and prove that we hold a particular account or whatever, it is something only you can do.

So what I would like to emphasize is that once this happens to somebody, the process for clearing it up is extremely long and extremely painful. So given the limited resources that we have, the need that we have to deal with this so quickly in light of the September 11 attacks, I think we are doing the right thing to focus on the prevention end right now. I mean, we will get to how to clear it up, how to create a system to help people overcome this problem. Right now, as I look back on my experience, I wish there was a more rigorous system that would prevent somebody from getting that information, from using it freely, from getting a fake identification card.

So I think at this point, we are doing the right thing. We are focusing on prevention and I hope that this panel and this system can do everything in its power to make this all stop.

So once again, thank you for the opportunity for coming here and it is an honor.

Senator DURBIN. Thank you. Nice haircut. [Laughter.]

Chief Viverette.

TESTIMONY OF MARY ANN VIVERETTE,[1] CHIEF OF POLICE, GAITHERSBURG, MARYLAND, ON BEHALF OF THE INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

Chief VIVERETTE. Good morning. I am pleased to be here today on behalf of the International Association of Chiefs of Police. As you may know, the IACP is the world's oldest and largest organization of law enforcement executives. It was founded in 1893 and with a current membership exceeding 19,000.

At the outset, I would like to thank you for holding this hearing today. From a law enforcement perspective, the importance of ensuring the integrity of identification documents cannot be overstated. Even prior to September 11, the IACP had been concerned with the availability of false identification documents and the ease in which false information could be used to obtain valid State-issued driver's licenses.

Law enforcement has seen that the ability of individuals to misidentify themselves can have serious, often tragic, repercussions in our communities. For example, teenagers often seek to obtain false identification documents so that they can purchase alcohol. As we all know, underage consumption of alcohol often has fatal results. The National Highway Traffic Safety Administration reports that in the United States, drivers between the ages of 16 and 21 account for just 7 percent of all drivers in this Nation, yet are involved in 15 percent of all alcohol-related fatalities.

Additionally, individuals who have had their license suspended or revoked in one State because of their failure to operate a vehicle in a safe manner have all too often been able to go to neighboring States and acquire a new license under false pretenses. As a result, these unsafe drivers are back on the roads of our communities. Law enforcement officers who may encounter such individuals will rely on their license to identify the driver's infraction history and will, therefore, be unaware of the driver's actual status.

Off the roadways, the ease with which criminals can fraudulently obtain a valid license or manufacture a counterfeit one greatly facilitates their ability to commit crimes involving identity theft and identity fraud. In addition, each year, law enforcement officers expend thousands of hours in efforts to properly identify criminal suspects who have misidentified themselves to police.

However, as we all realize, the events of September 11 greatly increase our need to ensure that the integrity of the driver's license issuance process is enhanced and that the ability of law enforcement officers to detect fraudulent licenses is improved. As the September 11 attacks demonstrated, the local police and other public safety personnel will often be the first responders to a terrorist attack. However, the role of the State and local law enforcement agencies is not limited to responding to these events. These agencies can and must play a vital role in the investigation and prevention of future attacks.

Across the United States, there are more than 16,000 State and local law enforcement agencies. These agencies and the 700,000 officers they employ daily patrol the streets of our cities and towns, and as a result, have an intimate knowledge of the communities

[1] The prepared statement of Chief Viverette appears in the Appendix on page 29.

they serve and have developed close relationships with the citizens they protect. These relationships provide State and local law enforcement agencies with the ability to effectively track down information related to terrorists. Often, State and local agencies can accomplish these tasks in a more effective and timely fashion than their Federal counterparts, who may be unfamiliar with the community and its citizens.

In addition, police officers on everyday patrol, making traffic stops, answering calls for service, performing community policing activities, and interacting with citizens can, if properly trained in what to look for and what questions to ask, be a tremendous source of intelligence for local, State, and Federal homeland security forces.

However, in order to maximize the capabilities of State and local law enforcement officers, it is vital that we improve the accuracy and ensure the validity of what has become the de facto means of identifying individuals in this country, their driver's licenses. Law enforcement officials must be able to act with certainty when dealing with citizens in our communities. We need to be certain that they are who their identification documents say they are and we need to be certain that the documents themselves are not counterfeit.

The effort to improve the accuracy of driver's licenses is so vital because of the simple fact that individuals with a valid driver's license will have greater success in staying off the radar screen of State and local law enforcement officials. As subsequent investigations have shown, the ability of the September 11 terrorists to obtain driver's licenses or State-issued identification documents greatly facilitated their operation within the United States.

For example, as we all know, on September 9, a trooper from my home State of Maryland pulled over Ziad Zamir Jarrah, one of the terrorists on Flight 93, which crashed south of Pittsburgh, for speeding on Interstate 95 north of Baltimore. During this traffic stop, Jarrah produced an apparently valid driver's license from the State of Virginia, and as a result, the stop proceeded in typical fashion. However, if Mr. Jarrah had been unable to produce a license or if he had produced a license that the trooper could have identified as fraudulent, then further investigation would have been warranted and perhaps future events would have taken a different course.

To address this crucial issue, the International Association of Chiefs of Police believes that several steps must be taken. First, certain minimum standards must be established that will help to ensure that information used to establish an individual's identity at the time they apply for the driver's license is valid and accurate and consistent from State to State.

Second, agreement should be reached among the States for the inclusion of both a unique identifier, such as a fingerprint, and anti-counterfeiting security devices in driver's licenses.

Third, States should be encouraged to link databases so that licensing agencies and law enforcement personnel in other States will be able to access an individual's criminal and motor vehicle traffic violation history in order to assist in the identification of potential criminal suspects or problem drivers.

Finally, the IACP believes that penalties for identity theft and identity fraud should be increased.

In conclusion, I would like to state that the ability of individuals to obtain inaccurate identification documents either through fraud or forgery has been an area of vital concern to law enforcement agencies throughout the Nation for a number of years. Unfortunately, it took the events of September 11 to catapult this issue to the forefront of national debate. It is the IACP's hope that action to remedy this critical situation can be taken in a timely fashion. We look forward to working with this Subcommittee, other Members of Congress, and our colleagues around the Nation in this effort.

Thank you for the opportunity to appear before you and I would be happy to answer any questions.

Senator DURBIN. Thank you for your testimony. I appreciate it very much. Mr. Varn.

TESTIMONY OF RICHARD J. VARN,[1] CHIEF INFORMATION OFFICER, STATE OF IOWA, ON BEHALF OF THE NATIONAL GOVERNORS ASSOCIATION

Mr. VARN. Thank you, Senator Durbin and fellow panelists, interested guests. I would like to start by saying I am representing both NASCIO, which is the National Association of State Chief Information Officers, as well as NGA today.

I need to begin by saying that neither organization has an official position directly on the subject of identity security or enhancing the driver's licenses or the life document systems. NGA does not see a need for Federal action at this time. It believes it is a State issue and the States need initially to have an opportunity to address it.

NASCIO and its members have a special interest in the information technology issues surrounding identity security and want and need to play a role in coordinating and an operational role in the design, development, and implementation of IT solutions and systems. That said, let me point out some of the things I think do need to be done, some of which I personally believe involved some Federal action. That is my own personal opinion, though.

Identity security is a critical component, and I will offer my own personal opinion separate from NGA or NASCIO's opinions.

Identity security is a critical component of ensuring accuracy and preventing fraud in the granting of privileges and benefits in many government programs and processes. Identity is like a critical junction point in the wiring of government and the information society. If a fault occurs and false positive or false negative identifications are made, real harm, ranging from financial crime, ruined reputations, exploitation of vulnerable children and adults, and violent crime can result. Without good identity security, the trustworthy and deserving can be denied and the dishonest and undeserving rewarded.

A common point of confusion in the discussion around identity is between the right to anonymity and the right to privacy. Privacy laws and constitutional protections are plentiful. Anonymity analogs are scarce. One reason for this is for most of human his-

[1] The prepared statement of Mr. Varn with attachments appears in the Appendix on page 35.

tory, we have not been anonymous. We have lived in close-knit communities and people have known us since birth. We have ridden on that assumption, that we knew each other, and our credit systems and our business transaction systems have depended on that for the last 50, 60, 70 years, when, in fact, that system had fallen apart.

The other reason anonymity is not commonly allowed is that it only works where behavior, status, age, or individually granted rights and privileges are not at issue. You have a right to be anonymous when you pay cash or maybe when you look at public records, but not when you are seeking a license, or a government benefit, writing a check, using credit, working with children or in a secure area, or buying protection from risk. The people that do the transactions need to know who you are. Who they share that information with is a privacy matter. It is not possible to be anonymous and get those rights and privileges in most cases.

The identity system on which we depend for most of our transactions is broken and is more likely to actually enable identity theft and fraud rather than prevent it. Sound security in the creation of authentication needs three parts: Something you know, something you have, and something you are. We often rely on one or two of these to establish identity and extend privileges and benefits. As a result, facts such as we heard earlier, such as Social Security number, address, and birthday, mother's maiden name, which cannot be adequately protected as secrets, are used to create identity.

It is not these facts or inability to keep them secret that is the problem. It is that we rely on them alone to establish identity. Moreover, we have grossly inadequate methods for creating and determining validity of the documents that comprise the "something you have" component. And finally, as was pointed out, with the exception of photos, we have not yet embraced a common and coordinated system of a biometric for presenting something you are.

Our identity system is broken, therefore, because the parts are broken. We lack adequate investment, infrastructure standards, and process in coordination and information sharing among the responsible government entities.

I would like to just point out what others have said by pointing out that I get on planes—our driver's license system is one of those parts that is broken—I get on planes with this identity right here. It happens to look like a driver's license, but it is my State ID card. I needed no more than being an employee of the State of Iowa to board every plane I have gotten on since September 11, an example of the problem we have with the security of the driver's license system.

Cyber security, homeland security, electronic commerce, compliance with many laws such as HIPAA and this whole issue of identity security are related and need a coordinated solution. However, that is not how these programs are being done or addressed. We are headed towards years of rework, retrofit, and the integration of stacks of ID cards and ID systems unless coordination occurs now.

There is a crying need for this and this coordination could take many forms. I have listed some of them for you in my written testi-

mony, such things as interstate compacts, committees such as this looking at how the government spending is taking place in the agencies and in the programs that you have already authorized and making sure that it is coordinated both inside the Federal Government and between and among levels of government.

I want to mention one other program that we are doing in Iowa that might be also part of the solution. It is a relatively simple and cheap effort to ensure that, what we call life documents are protected from illegal duplication or misuse. We have simply digitized all 11 million birth records from the State of Iowa since the 1890's. This system will allow the creation of an index and a process to reference that single electronic record as the real and unique record of a person's birth and databases can reflect when that is used in other life document issuing processes, and persons who are the subject of that record can find out when their birth record is being used to create identity.

Finally, I would like to point out a need for coordination for some Federal activity concerning the legal entry of people into our country. There is a hodge-podge of systems that need to be coordinated into a single system which mirrors and is integrated with these enhanced State and local life document systems. The Federal Government needs to have a document that shows the beginning, the duration, the course, and the end of a legal entrant's life into our country, regardless of whether they are just visiting or making America their new home.

The multiple Federal systems need to create a common electronic shared equivalent of a birth and death record. That common electronic record can be used by all levels of government in the same fashion as a normal birth and death record and would be the reference document for forms of identity and extension of privileges and benefits. Such a record for legal entrants could include a photo, biometric, statement and documentation of their life facts, such as name, date of birth, and so on. Even if different cards or processes stem from this one record, we will enhance the interoperability and efficiency of issuance systems and we will prevent fraud.

With that, I would conclude by saying that NASCIO, NGA, and my department, the Information Technology Department of Iowa, thank you for the opportunity to testify today and I will be happy to answer questions.

Senator DURBIN. Thanks very much, Mr. Varn. Senator Allen.

TESTIMONY OF HON. BARBARA P. ALLEN,[1] STATE SENATOR, EIGHTH DISTRICT, STATE OF KANSAS

Ms. ALLEN. Thank you, Senator Durbin. I appreciate the invitation to testify today.

I became interested in the issue of identity theft last December and January when I personally became a victim of bank fraud. I will not go into the details here today, but I can say that it was a very time consuming and frustrating and scary experience.

As I researched this issue in my own State of Kansas, I was stunned to learn how easy it is to obtain fraudulent identification

[1] The prepared statement of Ms. Allen with an attachment appears in the Appendix on page 53.

which is government issued in the form of driver's licenses and ID cards.

As we all know, reports of identity theft have increased significantly and exponentially in the United States and, of course, in my State of Kansas, in the last several years. Today, I regret to say that Kansas is one of the easiest States in the country in which to obtain false identification and to steal someone's identity.

Kansas is one of only a few remaining States that will provide any applicant an immediately-issued driver's license or ID card with no requirement of a Social Security number or any biometric information. We have no security measures in place to protect Kansans to ensure that the person applying for a driver's license or a non-driver's ID card really is that person. A simple photograph yields an instant permanent piece of government-issued identification.

Kansas currently requires a photograph, but no Social Security number or fingerprint, to get a driver's license or an ID card. The bill which I cosponsored at the beginning of the 2002 legislative session would amend State law so that all applicants for driver's licenses or ID cards would be required to submit their Social Security number and a biometric identifier, the most common of which would be a thumbprint, to obtain identification. Applicants would then receive a temporary license or ID card, and only after verification of the applicant's identity would a permanent piece of identification be issued.

In addition, today in Kansas you can receive an ID card and a driver's license concurrently and we would no longer allow that to happen. That would be prohibited.

The District Attorney's Office in Johnson County, which is part of the Kansas City metropolitan area and also near my Senatorial district, reports that cases of identity theft double every year. Identity theft in the City of Overland Park, where I live, have increased 100 percent in each of the last 2 years. In my county alone, this crime causes over $1 million annually in losses to retailers, credit card companies, and banks. These losses are passed on to the consumer in the form of higher costs for products and services.

Of course, the financial implications of identity theft are substantial, but they pale in comparison to the damage that can be done, including loss of life, when criminals steal our identities and use them for evil purposes on a broader scale.

I have attached to my testimony today an article by Governor Tom Ridge, Director of the Office of Homeland Security, who is encouraging governors and other State officials to take steps to improve the security and authenticity of driver's licenses. Governor Ridge recently urged governors attending a National Governors Association meeting to draft model legislation setting standards for more secure licensing procedures. By coming up with their own procedures, Governor Ridge said the governors would avoid having standards forced on them by Congress.

Driver's licenses are much more than a license to drive. They allow us to open bank accounts, to cash checks, to write merchants checks, and to step onto airplanes. They are the most widely used and accepted domestic document to verify a person's identity, but they are not reliable and they will not be reliable until we

strengthen the verification identity process before a license is issued.

As Americans, we have two choices. We can leave the current identification system as it is and risk the personal and financial security of private citizens, the finances of the business community, and the lives of fellow Americans, or we can improve the system.

Going through this experience in my own State of trying to get legislation passed which would strengthen the identification system for licenses and ID cards, I found that there are some who argue a personal identification system is, in fact, an evasion of privacy or a limitation on personal freedom, but only those who have something to hide will lose from providing proof positive that they are who they say they are. Identity cards, and that, in fact, is what driver's licenses are today, should be as close to foolproof as technology can make them to protect us.

S. 559 is not about invading Kansans' privacy. It is about preserving Kansans' privacy and protecting Kansans' security.

Senator Durbin, you mentioned the nationwide effort to coordinate activities and I want to comment about a question you raised in our invitation letter, which was what should the role of the Federal Government be in enhancing the reliability and security of the driver's license system. Based on my own experience in Kansas, I feel quite strongly that a national ID card is not the answer. Perhaps the role of the Federal Government should be two things. First of all, to set standards for more secure licensing procedures, and second, to offer financial incentives to States that take every step possible to ensure that government-issued identification is authentic.

Personally, I would welcome incentives from the Federal Government to help convince legislators in my State it is critical we improve the security and authenticity of driver's licenses in Kansas. Many of them still do not appreciate the magnitude of this threat to our personal safety and financial security.

I just wanted to comment in closing that this bill passed the Kansas Senate in March on a vote of 25 to 15. It passed out of the House Judiciary Committee and it is currently lingering in the House of Representatives, but I am still hopeful that we will get it passed this session. Thank you.

Senator DURBIN. Thank you. Ms. Serian.

TESTIMONY OF BETTY L. SERIAN,[1] DEPUTY SECRETARY FOR SAFETY ADMINISTRATION, PENNSYLVANIA DEPARTMENT OF TRANSPORTATION, ON BEHALF OF THE AMERICAN ASSOCIATION OF MOTOR VEHICLE ADMINISTRATORS

Ms. SERIAN. Good morning, Mr. Chairman. I am Betty Serian, Vice Chair of the American Association of Motor Vehicle Administrators, AAMVA. I want to thank you for the opportunity to speak this morning.

AAMVA is a nonprofit association representing DMV administrators and law enforcement officials throughout the U.S. and Canada. And let me tell you about a few Americans.

[1] The prepared statement of Ms. Serian appears in the Appendix on page 58.

Larry and Rita Beller, Edward and Alice Ramaeker spent their golden years traveling across the country. They were killed on a New Mexico highway by a repeat DUI offender. The driver, holding eight prior convictions from different States, was under the influence of alcohol and plowed head-on into the retirees' car.

Emeke Moneme, an Ohio resident, had his wallet stolen at the local gym. Within weeks of having his license disappear, Emeke discovered an identity thief had opened 13 fraudulent accounts in his name totaling $30,000 in bad credit debt. It took him months to straighten out his life.

Sara Clark, a schoolteacher, was killed after her flight was overtaken by terrorists and crashed into the Pentagon. Terrorists boarded her flight using a fraudulently obtained driver's license. Sara Clark shared this sad fate with more than 3,000 other Americans on September 11.

Larry and Rita Beller, Edward and Alice Ramaeker shared a list of DUI fatalities with more than 16,000 Americans every single year. And Emeke Moneme shares identity theft with hundreds of thousands of American victims.

A common thread to these tragedies? The driver's license. The driver's license has become the most requested form of ID in the United States and Canada. Financial institutions require it to open an account. Retailers ask for it when you write a check. And the airlines demand it of you before you board a plane.

The United States has more than 200 different valid forms of driver's licenses and ID cards in circulation. Each State and D.C. has different practices for issuing licenses. Individuals looking to undermine the system, whether it be a terrorist, a drunk driver, or an identity thief, shop around for licenses in those States that have become the weakest link.

In addition, the lack of standard security features on a driver's license allows individuals to exploit this system. This makes it difficult for law enforcement to verify the validity of a license from another State, not to mention the identity of the person who is holding that license. The situation is worsened by the availability of counterfeit driver's licenses and fraudulent documents, breeder documents, over the net and in underground markets.

We already maintain driving records. However, the country needs more effective tools to manage them. Problem drivers who obtain multiple licenses spread their bad driving history from State to State. They avoid detection, they avoid penalties, they avoid punishment. We need a system, such as the proposed Driver Record Information Verification System, to keep bad drivers off the road and save the lives of those who responsibly use the privilege to drive.

DMVs already exchange driver history on commercial drivers through the 1986 federally mandated Commercial Driver License Information System, also known as CDLIS, and within a 4-year period, CDLIS kept 871,000 potentially dangerous commercial drivers off the road.

The American public wants a more secure license and there are five ways we believe that Congress can help. Support minimum standards and requirements for each State that each State must adopt when issuing a license. Help DMVs identify fraudulent docu-

ments. Support an interstate network for confirming a person's driving history. Impose stiffer penalties on those committing fraudulent acts. And provide funding to make this happen, funding so that States can help ensure a safer America.

Based on a recent survey, the public expects you to help. Eighty-three percent of the respondents use their driver's licenses for purposes other than driving. Sixty-five percent think it is too easy to obtain a fake license or ID card. Seventy-seven percent of the respondents favor Congressional action to modify the licensing process and ID security.

For years, AAMVA has worked to strengthen the driver licensing process. Following September 11, Americans quickly learned how easily terrorists obtain driver's licenses. What is saddening is that it took this catastrophic event to heighten America's awareness of the importance of secure ID credentials.

We want to ensure that every driver has one license and one driving history and Congress can make that happen. When you can verify identity, we are certainly one step closer to preventing fraud, protecting privacy, and saving lives. Thank you very much for the opportunity to testify.

Senator DURBIN. Thank you, Ms. Serian. Mr. Goleman.

TESTIMONY OF BARRY GOLEMAN,[1] VICE PRESIDENT, PUBLIC SECTOR, AMERICAN MANAGEMENT SYSTEMS, INC.

Mr. GOLEMAN. Thank you, Mr. Chairman, for your leadership and the opportunity to be here today.

Senator Durbin, we at AMS believe that this Subcommittee is on exactly the right track by holding this hearing and advocating the development of a more secure driver's license. We believe technology can advance identification security while preserving our personal freedoms.

I work for American Management Systems of Fairfax, Virginia, and I have been involved for nearly 30 years at the State and Federal level in how licenses are issued and in the information systems that support that process. I started as a driver's license examiner in the State of California issuing licenses. I ran a motor vehicle office and I worked to implement the one standard Federal license program that we have today, the commercial driver's license. Before I came to AMS, I worked at AAMVA, where I built and operated the information systems for the exchange of commercial driver information. And I know from personal experience that the system can be attacked.

When I was an examiner, I was presented with counterfeit documents to obtain a license. I stopped people from stealing identities for the purpose of cashing stolen checks. I was even offered bribes of cash or sexual favors in exchange for issuing driver's license. For the record, I refused those attempted bribes. [Laughter.]

But unfortunately, not all employees do.

As has been described by others on the panel here today, we have learned that in the aftermath of September 11 that terrorists obtained multiple driver's licenses and ID documents from State

[1] The prepared statement of Mr. Goleman with an attachment appears in the Appendix on page 66.

motor vehicle agencies with ease, some using fraudulent documents or bribes.

Despite this security breach, there is encouraging news. This is a problem we can fix. With technology that exists today, we can stop the fraud and counterfeiting of State licenses. A model for the kind of Federal and State cooperative effort that is needed is a development of the licensing program to meet the requirements of the Commercial Motor Vehicle Safety Act.

In helping to develop the information systems for this licensing program, I have seen firsthand how State and Federal agencies can work together. With Federal funding made available, State licensing experts can adopt and implement new strict Federal standards. Do not let detractors tell you this cannot be done.

Your leadership and that of the others on this Subcommittee, however, is going to be necessary to make this happen. It is imperative that we improve the integrity of the driver's license to enable it to live up to its reputation as a reliable personal identification document. The reality is that, today, the license is the trusted de facto identification used by Americans to prove their identity within our borders. Retailers use them for cashing checks, banks for account verification, and airports for access to secure areas.

Our newly revealed security vulnerabilities demonstrate how important it is that the next generation of ID documents adhere to standardized security features and use the highest level of tamper-resistant technologies available. Biometrics, such as fingerprints or facial recognition, for example, can complete a positive one-to-one authentication of an individual to the card. Smart cards will also make the driver's license into a carrier of important data, including the biometric identifier on the card itself.

Used without improved verification techniques, however, these cards will be useless as secure, reliable forms of identification. I urge you to consider new technologies to ensure that people with counterfeit or false IDs will not be able to obtain better, more secure licenses.

The first step is a thorough verification of the individual's identity before he or she enters into the system. To accomplish this, State examiners must have access to the data that backs up the documents, such as birth records and immigration data. Today's web services technologies can verify information in multiple databases while protecting the personal information from unintended disclosure.

At AMS, we are currently working with Federal and State agencies in an effort to improve the basis for making identification decisions. Without improved identity verification, it is clear that we will not be able to achieve our goal of a more trustworthy document.

I would also like to draw your attention to the importance of preventing or deterring employee fraud. Just as I was occasionally offered bribes, today's examiners have their integrity challenged when criminals seek any path to obtain a valid State license. To detect and deter fraud, licensing administrators must rely on technology for internal auditing and business intelligence tools. These are tools commonly used today in the commercial world.

For example, States issue commercial licenses today according to Federal standards and it takes about 45 minutes to complete a required driving test. As a supervisor, I would be concerned about an examiner who issued a commercial license in only 10 minutes and I would want to investigate that transaction, but I cannot do that unless I have the data.

The steps I have outlined are not only necessary, but achievable with Federal, State, and private cooperation. With your leadership, we can achieve success in improving our identification systems and homeland security. I thank you and I look forward to your questions.

Senator DURBIN. Thank you very much, Mr. Goleman. Mr. Jansen.

TESTIMONY OF J. BRADLEY JANSEN,[1] DEPUTY DIRECTOR, CENTER FOR TECHNOLOGY POLICY, FREE CONGRESS FOUNDATION

Mr. JANSEN. Mr. Chairman, thank you for having us here. I wanted to say that there are a lot of debates on this in the public fora and I have met with some of the other people in this room today. A lot of the other fora are more prone to sound bites and do not necessarily advance a solution to the debate and I congratulate you for bringing together a lot of people who do offer positive solutions. All of the groups that I know of here and from what I have heard from the other testimony are all trying to reach actual solutions, and there is not a simple one-size-fits-all approach that is going to fix this and I look forward to working with many of the other people here in the future.

The Free Congress Foundation works with Eagle Forum, the Electronic Privacy Information Center, and the ACLU to head a loose ad hoc coalition of groups that are opposed to a national ID system. I would like to, with that in mind, indulge the Chairman to include a letter that EPIC asked me to have included in the record.[1]

Senator DURBIN. Without objection.

Mr. JANSEN. I would like to highlight some of our concerns briefly and then go into some other comments. The coalition that we are working with put a letter to President Bush on the AAMVA proposal. We oppose Federal funding for that proposal for a variety of reasons, the first of which is that a national ID system would not prevent terrorism. An ID card is only as good as the information that establishes the identity in the first place and there are other solutions that need to be done.

A national ID would depend on a massive bureaucracy that would limit our basic freedoms. There are problems there in terms of just what the identification is. It is not just necessarily an identification system, but it could easily become a data collection system and there are broader and complex issues that need to be addressed there which could also contribute to identity fraud.

A national ID system would be expensive and it would direct resources away from more effective counterterrorism measures.

[1] The prepared statement of Mr. Jansen appears in the Appendix on page 80.

[1] The letter submitted by Mr. Jansen for EPIC with an attachment appears in the Appendix on page 124.

There have been a lot of varying estimates on this proposal and there are lots of other proposals that might be done. We do not know what the costs and benefits of these are and we need not rush into some kind of a solution for that.

Our organizations believe very strongly that a national ID system would contribute to identity fraud and make it much more difficult to remedy instances when victims have suffered identity theft.

Americans have consistently rejected the idea of a national ID and limited the uses of data collected by the government. In the 1970's, both Presidents Nixon and Carter rejected the use of Social Security numbers as a uniform identifier because of privacy concerns. A national ID would be one-stop shopping for perpetrators of identity theft, who usually use Social Security numbers and birth certificates for false IDs.

Even with the biometric identifier, such as a fingerprint, on a national ID, there is no guarantee that individuals will not be identified or, more importantly, misidentified in error. The accuracy of biometric technology varies, depending on the type and implementation, and it would be more difficult to remedy identity fraud when a thief has a national ID card with your name on it but his biometric information.

As an example of some of the problems that might happen if we were to standardize some of these issues, the letter that I received from the Subcommittee here asking me to testify had my name spelled differently in the two different times that it mentioned my name. Again, I am sure there was no intent to defraud or anything else, but transposition errors can happen.

Senator DURBIN. It was a test. [Laughter.]

Mr. JANSEN. A national ID could require all Americans to carry an internal passport at all times. That would compromise our privacy, limit our freedom, and expose us to unfair discrimination based on national origin or religion. The national driver's license right now is not used for many of these purposes, but other speakers here are right that it is used more broadly, and the more it is linked with other purposes, the more it could be used and abused for other purposes.

If it is linked with, for example, our educational backgrounds, it will not be difficult to determine that I went to a parochial grade school and Jesuit high school that began with the word "Saint" and determine, therefore, that I am Catholic. We need to be very careful what a national identification system is that we are talking about and also how it might be linked and used with data collection.

In addition to the concerns that we raised in this coalition letter, the Federal Government already has a lot of authority to address some of these concerns. Richard Clarke, who is the chairman of the new Critical Infrastructure Protection Board, was quoted in *Wired* magazine recently as saying, "On the government systems side, we already have a lot of authority to use standards and enforce them. We have never done that."

What we need to do is for the Federal Government to focus on systems that are directly affected by the Federal Government. Another speaker here today made reference to a use of a mailing that

helped perpetuate identity fraud. The post office has a national change of address system that needs to be addressed for uses for identity fraud.

We also need to be concerned that standardizing these procedures across the States would truncate the discovery process during a period of great technological change. Some States might adopt different types of biometric identification or different types of systems, such as the one advocated by Senator Allen, that might be a best system. Even if we adopt what might be an overall best system now, there is no guarantee that that system would always be the best system, and by actually having different States adopting different standards, we have a way of comparing and contrasting which systems work and which ones do not and adopting the better systems more broadly.

In conclusion, I would just like to applaud the Subcommittee for taking an active role in such an important question. The development of new technologies, including biometrics, might be able to improve the quality of identification systems, but their capability should not be exaggerated. The focus of the Federal Government at this point should be to address the inadequacies of their own systems, such as the passport and INS systems, and again, I thank you again for this opportunity.

Senator DURBIN. Thank you, Mr. Jansen.

Mr. Jansen, let me ask you, you have undoubtedly flown since September 11 and have been asked to produce a photo ID at an airport, is that correct?

Mr. JANSEN. Yes.

Senator DURBIN. Do you have problems with that? Do you object to that?

Mr. JANSEN. To producing ID or a driver's license to getting on an airplane?

Senator DURBIN. Right.

Mr. JANSEN. No, not at all.

Senator DURBIN. Why?

Mr. JANSEN. I think that it is a good protection for Americans and it is also a private commercial enterprise, and if I choose not to do that, I do not have to, as opposed to a government ID or a government-imposed system where citizens do not have that choice.

Senator DURBIN. You are getting way ahead of me here. The airports, of course, now are under Federal jurisdiction and the standards that are being used at those airports are subject to Federal rule, and one of those standards which is ubiquitous is the presentation of a photo ID. I think most people would understand that that is the entry into the system, and as you said, that is not an unreasonable request that you verify that you are, in fact, Bradley Jansen with one "s" and that you are the person who purchased the ticket. So if that standard of proof is reasonable, what is wrong with making certain that it is accurate?

Mr. JANSEN. There is nothing wrong with making sure that that system is accurate, and again, I applaud the Subcommittee for addressing these in a much more constructive fora than we have debated these in the past.

Having a photo ID does not necessarily require a specific identification card. I have traveled using my passport as well as my driv-

er's license. For example, in the situation of the terrorists, one of the terrorists used a passport that was stolen, and when the initial list of alleged hijackers came out, it included the name of someone who had had his passport stolen, had reported it stolen, and the State Department itself did not keep a record of passports that were stolen.

Shunting responsibility to the States on this, I think would risk absolving the Federal Government for their responsibility in maintaining the accuracy and identification of the systems for which they should be responsible.

Senator DURBIN. That is a good point, and let me assure you that no matter what we say about driver's licenses and State IDs or other forms of identification, it is not at the expense of the Federal Government meeting its own obligation, whether it is through the passports or whatever source of Federal ID is used.

But I want to make it clear that this hearing is about State-issued driver's licenses, not a national ID, that the States will still have the authority to issue and revoke those driver's licenses. There is nothing in legislation we are considering that would take that authority away from the States. What I am trying to explore here is ways to make certain that on a national basis, we have an accurate, reliable standard so that if I present an Illinois driver's license and Senator Allen presents a Kansas driver's license at Reagan National Airport, that they know going in that it is more likely that they are accurate. That is all that we are seeking to do here and it is not to establish a national ID, which brings a whole range of other issues into this discussion.

Mr. Wern, let me start with you, if I might, in my questions. Senator Allen has been a victim of identity theft and so have I, about 2 years ago. I was lucky. I did not go through what you did, but I got a phone call at my home in Springfield, Illinois, one day. My wife was nearby and they said, "Well, Durbin, we finally caught up with you." And I said, "What are you talking about?"

They said, "Did you think you could get by making charges at Home Depot in Denver, Colorado, and not paying thousands of dollars that you owe us?" I said, "I have never been to a Home Depot in Denver, Colorado." "Oh, yes, you have. Is this your Social Security number?" They gave it to me. "And this is your mother's name?" "Yes." "Well, you had a Home Depot credit card and these charges were made and you have ducked it and we have finally caught you here in Springfield."

In fact, someone had stolen my identity and it took me, I think, about 2 months to finally go through the credit system and clear it up. And to their credit, no pun intended, it worked, and when it was all said and done, my record was cleared.

You went through a much longer, more involved, and obviously painful process, but ultimately, the person who did this was apprehended, is that correct?

Mr. WERN. Yes.

Senator DURBIN. How did that happen, do you know?

Mr. WERN. It was soon after he got a DUI from an Ohio State patrolman and was able to give my information and basically walk scot free from that. I think that the vigilance that they took after that event, both the Mansfield Division of the Ohio State Patrol

and the local Mansfield Police Department, they really focused their energies on catching this guy because he basically crossed the line.

That is not to say that other law enforcement was resistant to following up on these things. It is just hard to catch somebody unless they really do something that bold and visible. Most of the time, these things happen over the phone, they happen on the Internet, and it is just hard to track a person down.

Senator DURBIN. A curious situation, though, that he would be pulled over for a traffic offense, not have a driver's license, and be able to talk his way out of it.

Mr. WERN. Yes.

Senator DURBIN. That is what happened?

Mr. WERN. That is what happened.

Senator DURBIN. Did you have the assistance of any State or Federal agencies in this effort to clear up your identity theft?

Mr. WERN. Aside from law enforcement, there were two investigators working on the case. I contacted the FTC, which has jurisdiction over identity theft cases. Now, at least from a research perspective, they do gather data. I also contacted the Secret Service and the post office, because a lot of what he was doing would be considered mail fraud.

The agencies were responsive, but I ultimately came to the decision that this is the kind of problem that I can better deal with myself. Their response was, well, send us everything you have. You send them everything you have and it is very hard from their perspective, sitting in an office far away, to really approach it from a granular level and talk to the creditors and track the person down.

And also, there has to be thresholds. There are thousands of these cases out there, and at the time when I contacted those agencies, it was at the beginning stage and I do not think that the numbers were quite high enough nor the incidents serious enough. Those agencies have to prioritize their time.

But I think I probably could have looked to those agencies more. I think, in retrospect, I probably could have benefited more from their resources, but it became routine. I learned how to deal with it and I tackled it, I guess, in my own way.

Senator DURBIN. And as you said, as a lawyer, you know how to write a forceful letter.

Mr. WERN. Yes.

Senator DURBIN. Chief Viverette, have you worked the Highway Patrol for the State of Maryland, or at least enforced traffic?

Chief VIVERETTE. Within my community, yes, sir.

Senator DURBIN. And so when someone is pulled over and presents a driver's license, which is the first thing that you are asked for, what is normal in terms of verification at the site of the stop or the arrest when it comes to that driver's license?

Chief VIVERETTE. Sir, it is normal for us to use that document fair on its face unless we have a computer available to us where we can check that documentation. It may be that the computer is down and we have to believe that what we receive is fair on its face and write the citation.

Senator DURBIN. If the computer is working, what can you learn?

Chief VIVERETTE. Well, we can learn more about that individual and ask additional questions. Sometimes we will ask for a registration and we can compare the information. But it is not unusual to find tickets in a stolen vehicle where someone has provided false information. The car is stolen and the tickets are left in the car as the culprit leaves the vehicle behind.

Senator DURBIN. But you have a computer system that links you to the Maryland State Police, is that how it works?

Chief VIVERETTE. That is correct, sir. Not all the cars have computers, just the fortunate agencies that can afford them. You can run them through communications, but sometimes air traffic and a busy night precludes that, or the computer may be down, or you just get very specific information that the person is not suspended.

Senator DURBIN. Ms. Serian, let us talk about the system now. Assume that Chief Viverette has pulled someone over and gone into the State computer system to get some more information to see if that driver's license is valid. Does that, for example, if she picks someone's license from the State of Pennsylvania, does her Maryland system check with the State of Pennsylvania at that point?

Ms. SERIAN. Yes. I believe there is a nationwide system that can check on the driver's status of records through the State police systems. Ideally, in police officers' cars in any State, eventually, you should be able to pull up the photo so that would tell you then if that really is the person or is not. But once again, photos are not even commonplace on all licenses and the technology has not—it is not available, I guess I should say. It is advanced, but not available everywhere.

So yes, there are communication links that can allow those things to happen, and perhaps Mr. Wern's record would have been flagged. But in this case, it probably was not. In the case when it would be flagged, the local or State police officer would know that this is a potential fraud issue here.

Senator DURBIN. But the communication between States is critical in the world of interstate commerce.

Ms. SERIAN. The communication between States is very critical, especially, Senator, between DMVs and driver licensing organizations. We right now have a critical communication in terms of information for the commercial drivers. The Commercial Driver Licensing Information System provides not only a status, but also the driving histories that can be transferred from State to State.

That is a very good system, and that is why the AAMVA proposal also calls for a system that includes the Drivers Record Information Verification System so that driving records and the information that surrounds that driver or ID card holder can be transferred from State to State. That will, indeed, help local law enforcement officials.

Senator DURBIN. Of course, some of the things that we are in the process of putting into a piece of legislation include trying to make certain that the issuance of the driver's license in the first instance is valid, that the person does prove their identity going in.

I was recently interviewed by one of the television networks. They sent a reporter to the streets of Los Angeles with $150. It took her 2 hours to come up with something that looked like a driv-

er's license, and those of us who walk through airports know how closely those licenses are examined. People look at them quickly and off they go. I think it would be easy to counterfeit them under the current circumstances.

There has been talk here about a smart card, about more information and transfer. The idea, I guess, is if you can swipe a credit card and in a hurry determine whether or not there is any credit to be issued, the same thing could be true for driver's licenses in the future, is that correct?

Ms. SERIAN. Yes, it is. However, I would say that right now, we need to really focus on improving the driver licensing document as the product that needs improvement. What States may wish to do in the future are taking a driver's license and making it other things, including health care benefits, those types of things. Many States are researching those possibilities right now. But that really needs to be a State-to-State decision.

What we have is a system that is broken and a product that is not very reliable. So I would really encourage the Subcommittee to stay focused on improving the driver's license.

For example, this is not a valid Pennsylvania driver's license. I know it. It is a counterfeit. But it would be very difficult, and it is very difficult for the 16,000 police organizations throughout the country, or in California, as you mentioned, to know if that is a valid license or not. That is why minimum standards are an important thing to consider.

Senator DURBIN. Let me ask you this, Mr. Varn, because I thought you made some very important philosophical distinctions about anonymity and when you surrender it in our society. In the National Governors Association, how far along are you in discussing this issue?

Mr. VARN. Not very far along, Senator. I would say the governors are at the beginning of discussing this issue. The technologists are a little further along. NASCIO has been looking at this issue of identity security for some time and you will find a number of efforts in different States to improve identity security, but I would say the governors just started to examine it.

Senator DURBIN. In fairness, we are just starting to work on this bill, so I am not being critical of your lack of effort, but I think when we look at what has happened in the 7 months or so since September 11, we now realize this is going to be the coin of the realm in America. You are going to have to produce a photo ID, and the question is, is it reliable and is it accurate?

Senator Allen, in the State of Kansas, you have gone through this experience. What kind of political resistance have you run into in terms of making your process a little more accurate?

Ms. ALLEN. The issue has been the issue of loss of privacy and loss of personal freedom, and I guess it just depends on your perspective on the issue, but to me, we are protecting privacy and protecting security and it is really those people who have something to hide who do not want to verify their identity. Those people who do not have anything to hide, I think are happy to provide whatever means are necessary to prove their identification.

Senator DURBIN. I guess the privacy issue is the most important part of this conversation. How far can or should government go in

asking questions? As Mr. Varn mentioned, when you walk in and say, "I want to drive a car in this State," you have basically said, "I am part of your system now. What are the standards you use in your system? Do I have to take a test, have my photo taken, a thumbprint?" Whatever it happens to be, I have really voluntarily submitted myself to a system that has been established in the State.

I want to make it clear for the record that what we are trying to establish here in this legislation are the basic minimum standards of identification. Each State can then decide where they want to go in terms of additional information, and that is something that will be debated in Kansas or Illinois or Pennsylvania, as to what other information might be included in that card. But when Chief Viverette and her officers with the International Association of Chiefs of Police stop someone across America, there ought to be some basic standards that they can look to and say, we know that this is a valid Pennsylvania driver's license and this one is not because there are certain elements we are going to look for that are common to each and every one of them.

I might also add, it is interesting, if you would go to the City of Chicago on virtually any weekday morning, just south of Wacker Drive, you will see hundreds of people standing on the sidewalk outside of an office building. They are trying to get into the Mexican consulate because the country of Mexico is now issuing a card called a matricula and the matricula is a national ID card in Mexico, and these Mexicans in the United States are anxious to get it because with that card, they can get into the financial system in our country. They can open bank accounts and do other things.

The standard of proof for those cards is far beyond any driver's license that I have seen in the United States. They have to produce original copies and certified copies of birth documents, a copy of a driver's license, for example, from Mexico, local identification as well. It is a very high standard which is being used.

And it is interesting that we are saying to people from other countries in our Nation, you are held to this high standard, but yet for those within our Nation, we do not seem to establish the same standard of proof in terms of what we can achieve.

Mr. Goleman, let me ask you about the technology. You have talked about that for a second. How expensive is this? Where is this going to take us in terms of what it will cost to make these cards less easy to counterfeit?

Mr. GOLEMAN. The card production itself, States probably spend today in the neighborhood of about $1 per card to produce the current type of driver's license. Actually, Ms. Serian can probably tell you more accurately what she pays in Pennsylvania. But I would estimate that card production costs would probably go up substantially, up into the $2, $3, $4, $5 range in order to put much higher security features on the licenses, or if you go to smart cards or imbed biometric technology into the card itself. It is still not a high cost, more similar to the costs that Europeans pay for identity cards.

Senator DURBIN. The range of $1 to $5, you think, is a reasonable range for our conversation here in terms of current cost versus additional expense to make them more reliable?

Mr. GOLEMAN. Yes, I do. On a mass production basis, I think that the costs would be that.

Senator DURBIN. Senator Allen, did you want to comment on that?

Ms. ALLEN. Well, I did. In our bill, we originally doubled the fees for everything to cover the costs of implementation and there was a lot of resistance to that. So what we ended up doing was amending the bill and we just raised the photo fee by $1, from $2 to $3, and we estimated that that would cover the cost of implementing even the biometric piece. So it is really not a big increase.

Senator DURBIN. That takes that argument to a different level.

Let me ask you about the other question, about the use of databases by the States in issuance of driver's licenses. Getting back to the point Mr. Jansen and others have made about privacy here, can you tell me what you think the standard should be, should there be any national standard, let us say, about the use of the database of information beyond law enforcement and verification of identification? Ms. Serian.

Ms. SERIAN. There absolutely should be, Senator. Motor vehicle agencies right now are governed by some of the strictest privacy standards anywhere, and that is the Driver Privacy Protection Act. We take those very seriously. In fact, many States have even more stringent privacy regulations and laws than the DPPA requires. We take that very seriously and we certainly follow that law.

I do believe that with any new proposal, we should probably consider additional amendments or considerations to change the Driver Privacy Protection Act in terms of strengthening it even further. Even though we have very stringent privacy laws and regulations and we take those very seriously and we treat that as a great responsibility, I think there is still a need to even consider stronger amendments to the Driver Privacy Protection Act.

For an example, if I may——

Senator DURBIN. Sure.

Ms. SERIAN. An example of taking your license right now and not using it for verification procedures—this is a real Pennsylvania license here—and using it in bars or nightclubs, not just for verification of age, or in convenience stores for verification to be able to buy tobacco, taking that information that is on there and storing it, even though you might give it up freely to go into that bar, or even though you might give it up freely to go to the convenience store or stay in a hotel, I think we need to consider greater uses in terms of more stringent requirements so that it can only be used for verification purposes and certainly not retaining the data.

Senator DURBIN. Mr. Goleman, you also made a reference to Federal standards when it came to commercial driver's licenses. What are those standards that currently apply when the States issue these commercial driver's licenses, the Federal standards?

Mr. GOLEMAN. There are several standards. There are standards for the actual tests that the driver has to take. But as far as the information system goes, the States issue the licenses according to the Federal standards and the States maintain that driving record, but once they issue that license, they essentially register that driver into the Commercial Drivers License Information System, which

is merely an index of the fact that this driver, Joe Smith, with this date of birth and this driver's license number was issued a license in the State of Illinois.

If that driver attempts to get a license in any other State, the State is required to check first to see if he is already registered in the system, and if he is, then that record is pulled back into the new State for combining with his existing record.

So the States retain the data in their own systems. It is a very critical aspect of the system, that they retain ownership of that data and are responsible for it. Yet there is a centralized index that allows them to locate the record wherever it is.

Senator DURBIN. Good. Thank you very much.

I might say that we had a number of witnesses who wanted to join us today from a variety of different groups, Mothers Against Drunk Driving and others. Each group kind of came to this from a little different angle, but they all started with the same premise, that the misuse of driver's licenses had caused terrible problems, and I think we have heard about quite a bit of that today.

The identity theft question, which involves not just credit but traffic offenses and, in fact, reputation of an individual, which has to be reconstructed, and fortunately, Mr. Wern, you were able to do that because of your own skills.

Chief Viverette has talked to us about the law enforcement side of this. But for a driver's license issued to one of the would-be terrorists and used on September 9 to avoid any further investigation, people may be alive today who were killed on September 11. It is a matter of that sort of gravity.

We have also heard and probably know from personal experience these young people who use these driver's licenses for alcohol and tobacco and to hide bad driving records.

The list goes on and on, and I think it really calls on us to try to come up with a reasonable means of cooperating with the State issuing agencies so that we can establish meaningful standards so that people know that it is a serious process in the issuance of State IDs and driver's licenses so that we can verify that they are not defeating the system by forum shopping in different States for the easiest place to find a driver's license, so that we can also find out whether someone has a bad driving record in one State and is trying to avoid that knowledge in another.

It is a way to crack down on fake ID mills and to deter internal fraud, and I think Chief Viverette made the point, and others, as well, we need to stiffen the penalties. We need to take this seriously. If we are going to go through what I consider to be the acceptable hassle of producing photo IDs, let us make certain that they are accurate from the start.

Thank you all very much for joining us. It was a good panel and we will proceed in preparation of this legislation.

The Subcommittee meeting will stand adjourned.

[Whereupon, at 11:24 a.m., the Subcommittee was adjourned.]

APPENDIX

Theodore W. Wern
301 West Concord Place, Apt. 1
Chicago, Illinois 60614
Telephone: 312.337.8413
Email: theodore_wern@kirkland.com

April 16, 2001

Senator Richard J. Durbin
United States Senator, Illinois
332 Dirksen Senate Office Building
Washington, D.C. 20510

Re: A License to Break the Law? Protecting the Integrity of Driver's Licenses

Dear Senator:

I respectfully submit the following written testimony in connection with the following hearing held by the Senate Subcommittee on Oversight of Government Management, Restructuring and the District of Columbia: *A License to Break the Law? Protecting the Integrity of Driver's Licenses.*

I was a victim of identity theft for approximately four years. The perpetrator used my personal information to establish approximately $48,000 in fraudulent credit and for various other financial crimes. He also used that information in the course of his own traffic violations. On four separate occasions, he was stopped by traffic police -- once for driving under the influence of alcohol -- and was able to incur the violations under my identity. On another occasion, the perpetrator assumed my identity during a judicial proceeding resulting from one of his traffic violations. He was able to plead guilty and walk away from the courthouse while never having to reveal his own name. All along, his violations resulted in numerous arrest warrants issued under my driving record. My perpetrator is now serving a 6 month sentence in a state prison in Mansfield, Ohio.

I will not dwell on the anger and frustration that resulted from my experience. Certainly, such emotions pale in comparison to those that resulted from the events of September 11. As we all know, those events were set in motion by many individuals who were able to assume fraudulent identities. What I offer today is a basic awareness of the inadequacies of current administrative and law enforcement efforts to prevent identity theft.

The first remedial effort should be focused at the state agency level. As contemplated in the proposed draft of the Driver's License Integrity Act of 2002 ("DLIA"), *all states* should be forced to adopt more aggressive standards for the issuance of driver's licenses.

The second remedial effort should be aimed at law enforcement. What good is a validly issued driver's license if an identity thief can use *the information* contained in that

driver's license to commit crimes with impunity? In my case, three different city police officers (two of which were from different jurisdictions) and one state highway patrol officer failed to take any practical steps to ensure that the violator was who he said he was. Those officers only accepted the perpetrator's word that he was "me." No effort was made to confirm that identity, *even though* the perpetrator failed to show any identification and *even though* the perpetrator's physical appearance bears no resemblance to mine. Therefore, as contemplated in the DLIA, the effort should not end with uniform driver's license standards; rather, it should also extend to law enforcement officers and any other persons or entities who are charged with determining the validity of a person's identity.

Thank you for the opportunity to address this panel. I would be honored to provide any further service to the cause that brings us together today.

Sincerely

Theodore W. Wern

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

TESTIMONY

Statement of

Chief Mary Ann Viverette

4th Vice-President

Of the

International Association of Chiefs of Police

Before the

Subcommittee on Oversight of Government Management, Restructuring, & the District of Columbia

Committee on Governmental Affairs

United States Senate

April 16, 2002

515 N. WASHINGTON STREET
ALEXANDRIA, VA 22314
703-836-6767
WWW.THEIACP.ORG

Good Morning, Chairman Durbin, Senator Voinovich and members of the Subcommittee.

I am pleased to be here today on behalf of the International Association of Chiefs of Police. As you may know, the IACP is the world's oldest and largest organization of law enforcement executives, founded in 1893, and with a current membership exceeding 19,000.

At the outset, I would like to thank the Subcommittee for holding this hearing today. From a law enforcement perspective, the importance of ensuring the integrity of identification documents cannot be overstated. Even prior to September 11th, the IACP had been concerned with the availability of false identification documents and the ease in which false information could be used to obtain valid state-issued driver's licenses.

Law enforcement has seen that the ability of individuals to misidentify themselves can have serious, often tragic, repercussions in our communities. For example, teenagers often seek to obtain false identification documents so that they can purchase alcohol. As we all know, underage consumption of alcohol often has fatal results. The National Highway Traffic Safety Administration (NHTSA) reports that in the United States, drivers between the ages of 16 and 21 account for just 7 percent of all drivers in this nation, yet are involved in 15 percent of all alcohol-related fatalities.

Additionally, individuals who have had their license suspended or revoked in one state because of their failure to operate a vehicle in a safe manner have all too often been able to go to a neighboring state and acquire a new license under false pretenses. As a

result, these unsafe drivers are back on the roads of our communities. Law enforcement officers who may encounter such individuals will rely on the license to identify the drivers infraction history and will therefore be unaware of the drivers actual status.

Off the roadways, the ease with which criminals can fraudulently obtain a valid license or manufacture a counterfeit one greatly facilitates their ability to commit crimes involving identify theft and identity fraud. In addition, each year law enforcement officers expend thousands of hours in efforts to properly identify criminal suspects who have misidentified themselves to police.

However, as we all realize, the events of September 11th, greatly increased our need to ensure that the integrity of the driver license issuance process is enhanced and that the ability of law enforcement officers to detect fraudulent licenses is improved.

As the September 11th attacks demonstrated, the local police and other public safety personnel will often be the first responders to a terrorist attack. However, the role of state and local law enforcement agencies is not limited to responding to these events. These agencies can and must play a vital role in the investigation and prevention of future attacks.

Across the United States, there are more than 16,000 state and local law enforcement agencies. These agencies, and the 700,000 officers they employ, daily patrol the streets of our cities and towns and, as a result, have an intimate knowledge of the communities they serve and have developed close relationships with the citizens they

protect. These relationships provide state and local law enforcement agencies with the ability to effectively track down information related to terrorists. Often, state and local agencies can accomplish these tasks in a more effective and timely fashion than their federal counterparts, who may be unfamiliar with the community and its citizens. In addition, police officers on everyday patrol, making traffic stops, answering calls for service, performing community policing activities, and interacting with citizens can, if properly trained in what to look for and what questions to ask, be a tremendous source of intelligence for local, state and federal homeland security forces.

However, in order to maximize the capabilities of state and local law enforcement officers, it is vital that we improve the accuracy and ensure the validity of what has become the de facto means of identifying individuals in this country: their drivers' licenses. Law enforcement officials must be able to act with certainty when dealing with citizens in our communities; we need to be certain that they are who their identification documents say they are; and we need to be certain that the documents themselves are not counterfeit.

The effort to improve the accuracy of driver's licenses is so vital because of the simple fact that individuals with a valid driver's license will have a greater success in staying off the radar screen of state and local law enforcement officials. As subsequent investigations have shown, the ability of the September 11th terrorists to obtain driver's licenses or state issued identification documents greatly facilitated their operations with the United States.

For example, as we all know, on September 9th, a trooper from my home state of Maryland pulled over Ziad Zamir Jarrah, one of the terrorists on Flight 93 which crashed south of Pittsburgh, for speeding on Interstate 95 north of Baltimore. During this traffic stop, Jarrah produced an apparently valid driver's license from the state of Virginia, and as a result, the stop proceeded in typical fashion. However, if Mr. Jarrah had been unable to produce a license or if he had produced a license that the trooper could have identified as fraudulent, then further investigation would have been warranted and perhaps future events would have taken a different course.

To address this crucial issue, IACP believes that several steps must be taken.

First, certain minimum standards must be established that will help to ensure that information used to establish an individual's identity at the time they apply for a driver's license is valid and accurate and consistent from state to state.

Second, agreement should be reached among the states for the inclusion of both a unique identifier, such as a fingerprint, and anti-counterfeiting security devices in driver's licenses.

Third, states should be encouraged to link databases so that licensing agencies and law enforcement personnel in other states will be able to access an individual's criminal and motor vehicle traffic violation history

in order to assist in the identification of potential criminal suspects or problem drivers.

Finally, the IACP believes that the penalties for identity theft and identify fraud should be increased.

In conclusion, I would like to state that the ability of individuals to obtain inaccurate identification documents, either through fraud or forgery, has been an area of vital concern to law enforcement agencies throughout the nation for a number of years. Unfortunately, it took the events of September 11th to catapult this issue to the forefront of national debate. It the IACP's hope that action to remedy this critical situation can be taken in a timely fashion. We look forward to working with this Committee, other members of Congress, and our colleagues around the nation in this effort.

Thank you for the opportunity to appear before you today. I will be glad to answer any questions you may have.

Testimony before the Senate Subcommittee on Oversight of Government Management, Restructuring and the District of Columbia

A Hearing Regarding: A License to Break the Law? Protecting the Integrity of Driver's Licenses

Presented by Richard J. Varn, CIO, State of Iowa, on behalf of the National Association of State Chief Information Officers (NASCIO), the National Governor's Association (NGA), and the Information Technology Department (ITD), State of Iowa

April 16, 2002

Summary

Neither the NGA nor NASCIO have an official position directly on the subject of identity security or enhancing the driver's license and life document systems.

Identity security is a critical component of ensuring accuracy, preventing fraud, and granting privileges and benefits in many programs and processes.

Our identity system is broken and is more likely to actually enable identity theft and fraud rather than prevent it.

Our driver identity systems, cards, and issuance processes are not adequately coordinated to ensure transportation safety or the security of the myriad of their other uses on which we have come to depend.

Our life document systems for recording and providing proof of birth, marriage, name change, and death are inadequate to the task of supporting the issuance of identity and the extension of privileges and benefits. An enhanced life document issuance and verification system is essential to identity security.

Cyber-security, homeland security, secure electronic commerce, compliance with many laws such as HIPAA, and identity security are all related and need coordinated solutions.

Sound security in the creation and authentication of identity needs three parts: something you know, something you have, and something you are. We often rely on only one or two of these to establish identity and extend privileges and benefits. As a result, facts such as social security number, address, birth day, and mother's maiden name, which cannot be adequately protected as secrets, can be used to create identity and extend privileges and benefits fraudulently. It is not these facts or our inability to keep them secret that is the problem: it is that we rely on them alone to establish identity. Moreover, we have grossly inadequate methods of creating and determining the validity of life documents that comprise the "something you have" component. Finally, with the exception of photos, we have not yet embraced a common or coordinated biometric system for presenting "something you are".

The federal systems for legal entry of a person into our country need to mirror and be integrated with enhanced state and local life document and driver's license systems. The federal systems need to document the beginning, duration, course, and end of a legal entrant's "life" in our country regardless of whether they are just visiting or making America their new home. The multiple federal systems need to create a common, electronic, shared equivalent of a birth and death record. That common electronic record can be used by all levels of government in the same fashion as normal birth and death record and would be the referenced document for issuance of forms of identity and the extension privileges and benefits. Such a record for legal entrants could include a common photo, biometric, and the statement and documentation of their life facts such as name, date of birth, and so on. Even if different cards (driver's licenses, visas, etc.) were issued from this document, having the single common record would enhance security, prevent fraud, and increase the interoperability and efficiency of issuance and verification systems.

Addressing the issue of identity security is a process, not just a product. We are at the beginning of that process and it is recommended that mechanisms for ongoing input and consultation are needed on both technical and policy matters.

NASCIO members and the association itself play a critical role in coordination and implementation of federal, state, and local information technology systems and can be an invaluable resource for the federal government if given the opportunity. This is also true of the NGA, American Association of Motor Vehicle Administrators (AAMVA) and the National Association of Public Health Statistics and Information Systems (NAPHSIS) as well, just to name three of the many associations of state officials who stand ready and able to help. Private industry groups, such as the National Retail Federation (NRF), are also very interested in this

issue and are playing a role in ensuring that those who must check ID are represented in this discussion.

There are many federal, state, and local projects and programs that overlap, are not coordinated, and have a great potential for duplication, lack of interoperability, and incompatibility. There is a crying need for coordination at each level of government and between levels of government on identity security on technical standards and systems and in policy making. It is not yet clear what the best options or mix or options are for this coordination. Some possible choices include:

- Interstate compacts
- Intergovernmental agreements
- Standards development through recognized standards bodies
- Coordination of information technology system architecture, development, and operation
- Federal funding for enhanced life document systems and driver's license issuing processes, systems, and cards
- Legislative and executive coordination of the funding, development, enhancement, and implementation of identity security programs and systems within and among each level of government
- Establishment of a single point of contact and coordination for various federal initiatives
- Creation of formal or informal federal, state, and local groups to coordinate technical and policy activities and exchange information

The need for coordination, the importance and diversity of interests in identity security, and a spirit of cooperation were in evidence at an Identity Security Forum held in Washington, DC in March of 2002. The forum was co-sponsored by NASCIO, AAMVA, NAPHSIS, and NRF and was attended by representatives of many government entities and private sector interests. A summary of the proceedings is attached under separate cover.

Iowa is working on creating an identity security clearinghouse process to ensure that life documents are not misused, used in illegal duplicate fashion, nor used without the knowledge of the subject of the document. A summary of this project is included with this testimony.

NASCIO, NGA, ITD, and I thank you for the opportunity to provide input on this critical issue.

Identity-Security Clearinghouse

Iowa Information Technology Department

Version 1.0
2/8/2002

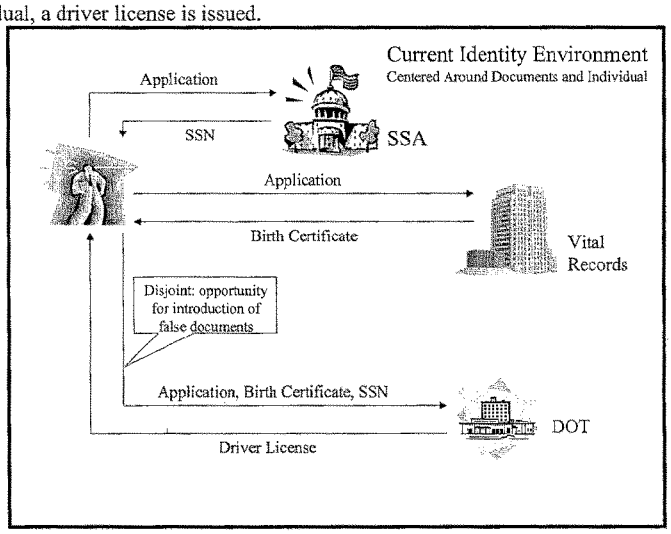
http://www.infoweb.state.ia.us/ecomdev/current_projects/identity/index.html

Existing Identity Security Environment

There exists today an identity-security infrastructure that relies heavily on identity documents issued by a variety of agencies and organizations. This infrastructure consists of the processes, personnel, and security requirements of each of the issuing entities. The identity documents are then given to the individual as a symbol to other entities that use the document for identification purposes. For example, once you receive your birth certificate, you can receive your Social Security Card, and then in the future present these for a number of other permissions such as your driver's license or school enrollment.

The system has mostly relied on the integrity of the individual presenting the document as opposed to relying on the issuing entity of the identity indicia. For example, a clerk at a driver license issuing station may recognize a presented birth certificate as having the same size, shape, color, wording and stamp as an Iowa birth certificate but unless that can be verified back to the issuing entity the presented document is nothing more than a piece of paper. Therefore the reliance on the individual leads to a disjointed identity system that can easily be abused or circumvented.

The exhibit below demonstrates this based on a scenario for applying for a driver license. The applicant at birth received both a birth certificate and a social security number on a card. Both of those identity indicia can be used for the issuance of a driver license. Since there is a reliance on the judgment of the agent viewing the documents it is easy to see the point in the process where an individual could obtain false documents and present them for the driver license. If there is no reason for doubt of the documents and the individual, a driver license is issued.



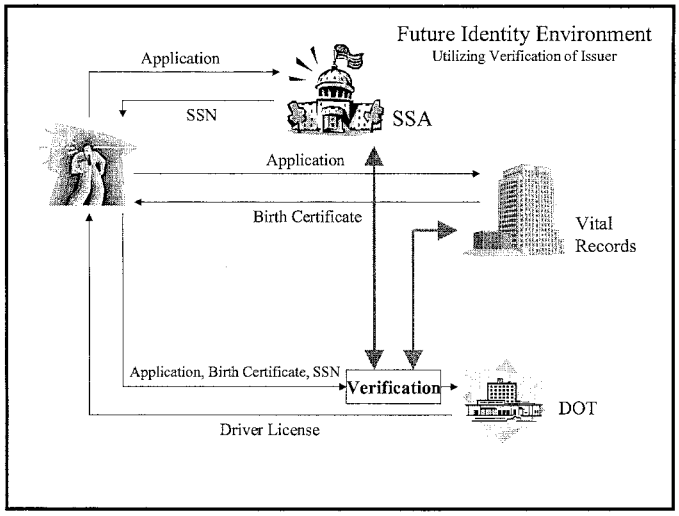
Recent Events

This disjointed process relying on paper and individuals creates a system that is primarily reactive and only reacts when disaster occurs. In other words, if a person can circumvent the identity system and create a false identity it may go unnoticed if the person does not do anything to draw attention to them.

The events of September 11, 2001 have raised quite a number of issues concerning identity theft. The terrorists reportedly used assumed identities to gain access to funds, training and the planes used in the attack. The end result is a sense of urgency surrounding all security issues including the accurate verification of a person's identity.

Future Identity-Security Environment

For the identity-security environment to improve, the processes for issuing identity documents need to be linked to provide verification of the documents. The previous illustration could be modified in the driver license scenario to include a layer of verification.

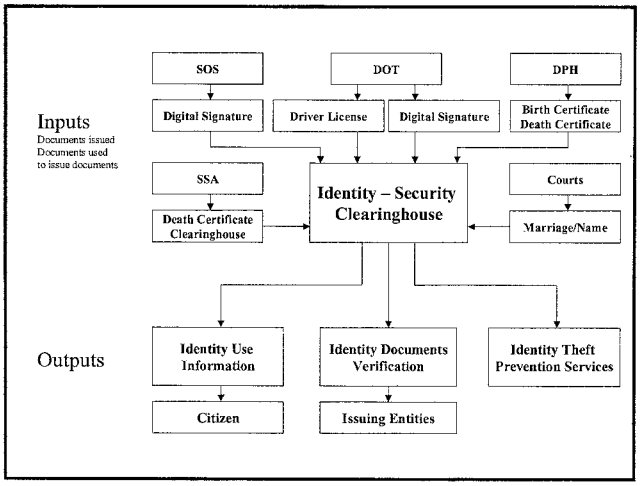


The above example incorporates the concept of identity verification where the DOT would verify the authenticity of the documents and the identification information on those documents. Verification would eliminate the use of falsified documents, and other problems that can arise when there is a disjointed system of identity. The ITD has been working to consolidate this continuous concept of identity into an Identity-Security

Clearinghouse that would perform the verification and minimize the load on the issuing entity.

Identity-Security Clearinghouse Concept

The Identity-Security Clearinghouse will link the documents used to create identity. These documents will include social security cards from the SSA, birth and death records from the DPH, driver's licenses and ID cards from the DOT, court filings such as marriage and name change filings affecting identity, and other identity documents. Identity rules and standards would be developed to ensure proper identity use.



Initial discussions on the Identity-Security Clearinghouse concept have centered on ensuring that only one legitimate birth certificate will be used to issue each social security number and each driver's license/ID. At the point of issuance for a social security number and DOT-issued driver's license/identity card (hereafter called ID), the birth certificate presented as proof of identity could be referenced against a state birth certificate database. If the birth certificate is valid and no other ID's have been issued from it, the birth certificate would be linked to ID's issued from it. The birth certificate record would also be electronically tied to the DOT photo database.

This has three advantages:

- When an ID is then presented in certain situations calling for strict security, a check could be run against the face database stored by DOT and identity could be established. (i.e. airport counter)
- Only one ID would be issued per birth certificate. This would allow easier identification of individuals attempting to falsify identity if the birth certificate is presented a second time.

- Enhanced procedures will lead to a decline of identity theft and fraud.

For residents outside of the State of Iowa, the birth certificate could initially be scanned at the point of issuance to tie it to the picture ID. (As standards are adopted for vital records databases and such databases are completed, the records would be linked in the same way as in-state records.) The basic information would be captured and indexed to cross reference against future ID issuances from the same birth certificate.

The end result would be a system that incorporates individuals, picture ID, processes, documentation, and identity. The current system does not link these components and makes identity theft too easy. Future stages would include establishing a national clearinghouse for death records that any jurisdiction could reference.

Identity-Security Benefits

The initial benefits of the Identity-Clearinghouse concept directly effect authentication methods within the State of Iowa:

- Enforcement of the 1:1 relationship between identity indicia will increase the reliability and integrity of the identity system.
- Standard methods for verifying identification will decrease the need for entities to develop their own method.
- There is potential for decreasing identity theft and fraud with State programs.

The development of an Identity-Clearinghouse also has benefits for the State of Iowa in improved customer service and enterprise data sharing.

- Digital signature implementation will bring State agencies into a "circle of trust" that will facilitate shared user authentication across multiple agencies facilitating portal growth.
- Identity data standards will allow the State of Iowa to formalize programming standards reducing development time.
- Identity standards will provide a common format for the sharing and security of information between State agencies where such sharing is permitted.
- The Identity-Clearinghouse could serve as a national model and become the one point of coordination for the State of Iowa with a federal national ID effort.

Current Status of the Iowa Project

The following actions have occurred:

- The DOT and DPH are creating a system for verifying Iowa birth certificates
- DOT is participating in AAMVA discussions on identity standards
- DPH has indexed and imaged approximately 11 million birth certificates going back to the 1890's
- ITD has facilitated a conversation between DOT, DPH, DPS, and the Social Security Administration to discuss common needs and identify future direction.

Next Steps in Iowa Project

Actions associated around this implementation of the Identity-Security Clearinghouse:

- Evaluation of documents, standards, and procedures used by issuing authority used by the DOT to confirm and establish identity. (i.e. primary and secondary documents)
- Coordination between DOT and DPH to tie individual birth certificates to an individual driver license.
- Further coordination to tie individual death certificates to the ID revocation process.
- Establishment of a history trailer for ID and related documents such as birth certificates to allow the citizen to track issuances of and requests of their ID.
- Coordination of the ability to access the DOT face database to confirm the photo ID where appropriate and allowed.
- Further development of the driver license to contain and access a unique identifier such as a PKI certificate and other biometric data.
- Consideration of a pilot to allow criminal justice, DPH, and other state agencies real-time access to the Social Security Administration.
- Align the DPH birth certificate database with national standards being developed by the National Vital Records Association and NAPHSIS.
- Instituting a timely electronic filing of death notices to the DPH and SSA
- Establishing a national clearinghouse for death and birth information.

Once these modifications have taken place, the following needs to occur:

- Adoption of identity standards (i.e. policies, procedures, and implementation) for an enterprise to secure its systems.
- Digital signature implementation based on identity standards and with the scope of Iowa Code Chapter 554D.
- Implementation of technology and policies for use of identity at secure facilities (e.g. airports).
- Implementation of Iowa Code 18.138 (Government Services Card) through the improved Iowa Drivers License/PKI systems.
- Explore the possibility of the DOT and Secretary of State becoming the issuer of PKI digital certificates.

Related actions:

- Creation of an Identity Theft Advocate in the Office of the Attorney General. This Office would help victims of identity theft and have the authority to verify their claims and through affidavits and other mechanisms, repair the credit history and reputation of the victim.

For More Information:
http://www.infoweb.state.ia.us/ecomdev/current_projects/identity/index.html

Contact Information for Identity Security Forum

Name: Robert Adelardi
Title: CIO
Department:
Organization or Agency: Puerto Rico General Courts Adm.
Street Address: P.O. Box 190917
City: San Juan
State: Puerto Rico
Zip Code: 00919-0917
Phone: (787) 641-6962
Fax: (787) 250-1080
E-mail: roberta@tribunales.gobierno.pr

Name: Ann Beauchesne
Title: Program Director, Emergency Management
Department: Center for Best Practices
Organization or Agency: National Governors Association
Street Address: 444 N. Capitol Street, Suite 267
City: Washington
State: DC
Zip Code: 20001
Phone: (202) 624-5370
Fax: (202) 624-5313
E-mail: abeauchesne@nga.org

Name: Larry Bray
Title: Program Manager
Department: Strategic Information Security
Organization or Agency: Georgia Technology Authority
Street Address: 100 Peachtree, Suite 2300
City: Atlanta
State: GA
Zip Code: 30304-3404
Phone: (404) 463-7379
Fax:
E-mail: lbray@gta.ga.gov

Name: Jim Brown
Title: Washington Director
Department: Intergovernmental
Organization or Agency: CSG
Street Address: 444 N. Capitol St., NW #401
City: Washington
State: DC
Zip Code: 20001
Phone: (202) 624-5460
Fax: (202) 624-5452
E-mail: jbrown@csg.org

Name: Holly Calhoun
Title: Program Director
Department:
Organization or Agency: American Automotive Leasing Association
Street Address: 1191 N. Fairfax St., Suite 425
City: Alexandria
State: VA
Zip Code: 22314
Phone: (703) 548-0777
Fax: (703) 236-1949
E-mail: hollycalhoun@aol.com

Name: Rich Carter
Title: Director, IT Committee Services
Department: IT Committee Services
Organization or Agency: AAMVAnet
Street Address: 4301 Wilson Blvd., Suite 400
City: Arlington
State: VA
Zip Code: 22203
Phone: (703) 908-8296
Fax: (703) 908-2868
E-mail: rcarter@aamva.org

Name: Steve Cooper
Title: Senior Director for Information Integration and CIO
Department: Office of Homeland Security
Organization or Agency: Exec. Office of the President
Street Address: The White House, EEOB 176
City: Washington
State: DC
Zip Code: 20502
Phone: (202) 456-7531
Fax:
E-mail: scooper@who.eop.gov

Name: Linda Dodd-Major
Title: Counsel
Department: Executive Associate Commissioner/ Programs
Organization or Agency: US INS
Street Address: 425 I St., NW Suite 3034
City: Washington
State: DC
Zip Code: 20536
Phone: (202) 305-2529
Fax: (202) 305-2523
E-mail: linda.dodd-major@usdoj.gov

Name: Don Gilbert
Title: SVP, Information Technology
Department: Information Technology
Organization or Agency: National Retail Federation
Street Address: 325 7th Street NW #1100
City: Washington
State: DC
Zip Code: 20004
Phone: (202) 626-8126
Fax:
E-mail: gilbertd@nrf.com

Name: Dale Good
Title: CIO, Judicial Branch
Department:
Organization or Agency: MN Supreme Court
Street Address: Suite 145, MN Judicial Court
City: St.Paul
State: MN
Zip Code: 55155
Phone: (651) 297-7636
Fax: (651) 297-7595
E-mail: dale.good@courts.state.mn.us

Name: Bert Harberson
Title: Policy Director
Department:
Organization or Agency: CSG
Street Address: 2760 Research Park Drive
City: Lexington
State: KY
Zip Code: 40578
Phone: (859) 244-8000
Fax: (859) 244-8001
E-mail: bharberson@csg.org

Name: Neal Hutchko
Title: Policy Analyst
Department:
Organization or Agency: National Association of State Auditors, Comptrollers Treasurers
Street Address: 444 North Capitol St. NW, Room 234
City: Washington
State: DC
Zip Code: 20001
Phone: (202) 624-5451
Fax: (202) 624-5473
E-mail: nasactnh@sso.org

Name: Eva Kleederman
Title: Policy Analyst
Department: OMB
Organization or Agency: Office of Information Regulatory Affairs
Street Address: 725 17th St. NW
City: Washington
State: DC
Zip Code: 20503
Phone: (202) 395-3647
Fax: (202) 395-5167
E-mail: eva.kleederman@omb.eop.gov

Name: Matt Lathrop
Title: Director, Commerce & Economic Development Taskforce
Department:
Organization or Agency: The American Legislative Exchange Council
Street Address: 910 17th St., NW, 5th Floor
City: Washington
State: DC
Zip Code: 20006
Phone: (202) 466-3800
Fax: (202) 466-3801
E-mail: mlathrop@alec.org

Name: Morgan Long
Title: Telecom & Information Technology
Department: Policy & Legislation
Organization or Agency: ALEC
Street Address: 910 17th St. NW, 5th Floor
City: Washington
State: DC
Zip Code: 20006
Phone: (202) 466-3800 ext. 246
Fax: (202) 466-3801
E-mail: mlong@alec.org

Name: Phillip Loranger
Title: Ch Access Enabling Technology (Bio/smart card/PKI)
Department: DOT/FAA
Organization or Agency: FAA/ Go Team Load TSA
Street Address: 400 7th St. SW
City: Washington
State: DC
Zip Code: 20591
Phone: (202) 366-1066
Fax:
E-mail: Phillip.Loranger@faa.gov

Name: Ted Mason
Title: Director, EPS Network Services & Emerging Technologies
Department:
Organization or Agency: Food Marketing Institute
Street Address: 655 15th, NW Suite 700
City: Washington
State: DC
Zip Code: 20170
Phone: (202) 220-0735
Fax: (202) 220-0877
E-mail: tmason@fmi.org

Name: Jay Maxwell
Title: President, COO
Department:
Organization or Agency: AAMVAnet
Street Address: 4301 Wilson Blvd., Suite 400
City: Arlington
State: VA
Zip Code: 22203
Phone: (703) 522-1300
Fax: (703) 522-1553
E-mail: jmaxwell@aamva.org

Name: Kymberly Messersmith
Title: CEO, KM Strategies, Inc./ Executive Director, Credit Card Coalition
Department:
Organization or Agency:
Street Address: 106 S. Columbus St.
City: Alexandria
State: VA
Zip Code: 22314
Phone: (703) 548-1121
Fax: (703) 548-1128
E-mail: ksm@kmstrategies.com

Name: John G. Moore
Title: Program Analyst
Department: Office of Electronic Government
Organization or Agency: GSA
Street Address: 1800 F. St., NW, Room G-135
City: Washington
State: DC
Zip Code: 20405
Phone: (202) 208-7651
Fax: No
E-mail: Johng.moore@gsa.gov

Name: Michael B. Neale
Title: Senior Management Advisor
Department: Judicial Information Systems
Organization or Agency: Maryland Judiciary, Administrative Office of the Courts
Street Address: 266 Riva Rd., Suite 900
City: Annapolis
State: MD
Zip Code: 21401
Phone: (410) 260-1102
Fax: (410) 260-1112
E-mail: michael.neale@courts.state.md.us

Name: Mary Alice Noyes
Title:
Department: Fraud Prevention Programs
Organization or Agency: US Dept. of State
Street Address:
City: Washington
State: DC
Zip Code: 20520-4818
Phone: (202) 663-2568
Fax: (202) 663-2612
E-mail: noyesma@state.gov

Name: Stuart K Pratt
Title: VP Government Relations
Department:
Organization or Agency: Consumer Data Industry Association
Street Address: 1090 Vermont Ave., Suite 200, NW
City: Washington
State: DC
Zip Code: 20005
Phone: (202) 408-7416
Fax:
E-mail: spratt@CDIAonline.org

Name: Leslie Reynolds
Title: Executive Director
Department:
Organization or Agency: National Association of Secretaries of State
Street Address: 444 N. Capitol Street NW #401
City: Washington
State: DC
Zip Code: 20001
Phone: (202) 624-3525
Fax: (202) 624-3527
E-mail: reynolds@sso.org

Name: Maureen Riehl
Title: Vice President, State & Industry Relations Counsel
Department: Government Relations
Organization or Agency: National Retail Federation
Street Address: 325 7th Street, #1100
City: Washington
State: DC
Zip Code: 20004
Phone: (202) 626-8121
Fax: (202) 626-8198
E-mail: riehlm@nrf.com

Name: Thom Rubel
Title: Director, State Information Technology Programs
Department: Center for Best Practices
Organization or Agency: National Governors Association
Street Address: 444 N. Capitol Street #267
City: Washington
State: DC
Zip Code: 20001
Phone: (202) 624-7740
Fax: (202) 624-5313
E-mail: trubel@nga.org

Name: Eric M. Seabrook
Title: General Counsel
Department: Ohio Secretary of State
Organization or Agency: NECCC/NASS
Street Address: 15th Floor, 180 E. Broad St.
City: Columbus
State: OH
Zip Code: 43215
Phone: (614) 995-2170
Fax: (614) 995-5395
E-mail: eseabrook@sos.state.oh.us

Name: Pamela Sederholm
Title: Executive Director
Department:
Organization or Agency: American Automotive Leasing Association
Street Address: 1199 N. Fairfax St., Suite 425
City: Alexandria
State: VA
Zip Code: 22314
Phone: (703) 548-0777
Fax: (703) 236-1949
E-mail: AALAFleet@aol.com

Name: Helena Sims
Title: Senior Director, Public Private Partnerships
Department:
Organization or Agency: NACHA
Street Address: 13665 Dulles Technology Dr.
City: Herndon
State: VA
Zip Code: 20171
Phone: (703) 561-3930
Fax: (703) 787-0996
E-mail: hsims@nacha.org

Name: Judith Spencer
Title: Chair, Federal PKI Steering Committee
Department: Office of E-Government
Organization or Agency: GSA
Street Address: 1800 F. Street NW
City: Washington
State: DC
Zip Code: 20405
Phone: (202) 208-6576
Fax: (202) 501-6455
E-mail: judith.spencer@gsa.gov

Name: Molly Stauffer
Title: Committee Director
Department: Task Force on Protecting Democracy
Organization or Agency: National Conference of State Legislatures
Street Address: 444 North Capitol St, NW Suite 515
City: Washington
State: DC
Zip Code: 20001
Phone: (202) 624-3584
Fax: (202) 737-1069
E-mail: molly.stauffer@ncsl.org

Name: Tim Stephens
Title: Director, Education
Department:
Organization or Agency: NAPHSIS
Street Address: 1220 19th St., NW, Suite 802
City: Washington
State: DC
Zip Code: 20036
Phone: (202) 463-8851
Fax: (202) 463-4870
E-mail: tstephens@naphsis.org

Name: Jeanette Thornton
Title: Policy Analyst
Department: Office of Management
Organization or Agency: Information Policy/Technology
Street Address: 725 17th St. NW
City: Washington
State: DC
Zip Code: 20503
Phone: (202) 395-3562
Fax: (202) 395- 5167
E-mail: jthornton@omb.eop.gov

Name: Richard Varn
Title: CIO
Department: Information Technology Department
Organization or Agency: State of Iowa
Street Address: Level B Hoover Building
City: Des Moines
State: IA
Zip Code: 50319
Phone: (515) 281-8699
Fax: (515) 281-6137
E-mail: richard.varn@itd.state.ia.us

STATE OF KANSAS

BARBARA P. ALLEN
SENATOR, EIGHTH DISTRICT
JOHNSON COUNTY
P.O. BOX 4042
OVERLAND PARK, KANSAS 66204
(913) 384-5294
STATE CAPITOL, ROOM 120-S
TOPEKA, KANSAS 66612-1504
(785) 296-7353

TOPEKA
SENATE CHAMBER

COMMITTEE ASSIGNMENTS
CHAIR: ELECTIONS AND LOCAL GOVERNMENT
MEMBER: ASSESSMENT AND TAXATION
EARLY CHILDHOOD DEVELOPMENT SERVICES
FINANCIAL INSTITUTIONS AND INSURANCE
REAPPORTIONMENT

April16, 2002

Subcommittee on Oversight of Government Management, Restructuring, and the District of Columbia

"A License to Break the Law? Protecting the Integrity of Driver's Licenses"

Mr. Chairman, Members of the Committee:

Thank you for the invitation to testify before you today. I became interested in the issue of identity theft last December and January when I personally became a victim of bank fraud. As I researched the issue in my own state, I was stunned to learn how easy it is to obtain fraudulent, government-issued identification in Kansas, in the form of driver's licenses and non-driver's i.d. cards.

Reports of identity theft have increased exponentially in the United States, and in Kansas, over the last several years. American citizens, financial institutions, retailers, and credit card companies are the victims of this crime.

Today, I regret to say, Kansas is one of the easiest states in the nation in which to obtain false identification, and to steal someone's identity. There are no security measures in place to protect Kansans, to ensure the person applying for a driver's license or nondriver's i.d. card really is that person. A simple photograph yields an instant, permanent piece of government-issued identification.

Kansas currently requires a photograph, but no social security number, or fingerprint, in order to obtain a driver's license or non-driver's i.d. card. Senate Bill 559 would amend state law so that all applicants for driver's licenses and nondriver's i.d. cards would be required to submit their social security number and a biometric identifier, such as a thumbprint, to obtain identification. Applicants would receive a temporary license or i.d. card, and only after verification of the applicant's identity, would a permanent identification be issued.

The District Attorney's office in Johnson County, which is part of the greater Kansas City metropolitan area and near my senatorial district, reports cases of identity theft more than doubling every year. Identity theft cases in the city of Overland Park, where I live, have increased 100% in each of the last two years. In our county alone, this crime causes over $1 million annually in losses to retailers, credit card companies, and banks. These losses are passed on to the consumer in the form of higher costs for products and services.

The financial implications of identity theft are substantial, but they pale in comparison to the damage that can be done - including loss of life - when criminals steal our identities and use them for evil purposes on a broader scale.

An article I have attached to my testimony notes that Governor Tom Ridge, Director of the Office of Homeland Security, is encouraging governors and other state officials to take steps to improve the security and authenticity of driver's licenses. Ridge recently urged governors attending a National Governors Association meeting to draft model legislation setting standards for more secure licensing procedures. By

coming up with their own procedures, Ridge said, the governors would avoid having standards forced on them by Congress.

Driver's licenses are much more than a license to drive - they allow us to open bank accounts, cash checks, write merchants checks, and step onto airplanes. They are the most widely used and accepted domestic document to verify a person's identity, but they are NOT reliable. And they won't be reliable until we strengthen the identity verification process before a license is issued.

As Americans, we have two choices. We can leave the current identification system as is - risking the personal and financial security of private citizens, the finances of the business community, and the lives of fellow Americans - or we can improve the system.

Some argue a secure personal identification system is an invasion of privacy or a limitation of personal freedom. But only those who have something to hide will lose from providing proof positive they are who they say they are. Identity cards - and that is what driver's licenses are today - should be as close to fool-proof as technology can make them to protect us. S.B. 559 is not about invading Kansans' privacy, it's about preserving Kansans' privacy, and protecting Kansans' security.

What should the role of the federal government be in enhancing the reliability and security of the driver's license system? Based on my experience in Kansas, a national i.d. card is not the answer. Perhaps the role of the federal government should be 1.) to set standards for more secure licensing procedures, and 2.) to offer financial incentives to states that take every step possible to ensure that government-issued identification is authentic. Personally, I would welcome incentives from the federal government to help convince legislators in my state it is critical we improve the security and authenticity of driver's licenses in Kansas. Many of them still don't appreciate the magnitude of this threat to our personal safety and financial security.

Thank you Mr. Chairman. I will be happy to stand for questions.

FCWCOM
YOUR GOVERNMENT IT RESOURCE

HOME | FEDERAL COMPUTER WEEK | GOVERNMENT E-BUSINESS | TECHNOLOGY | EVENTS | LINKS | DIRECTORY |

SEARCH THE SITE
go
Advanced Search

ALSO ONLINE
Agenda
Letters Archive
Online Archive
Print Editions
Special Reports
Milt Zall Archives

NEWS BY TOPIC
Accessibility
CIOs
City
Columns
County
Defense
Democracy
E-Government
Funding
Homeland Defense
Industry
Intergovernmental
International
Policy
Privacy
Procurement
Records Management
Schools
Seat Management
Security
State
Technology
Telecom
Training
Workforce

READER SERVICE
Advertise
Contact us
Editorial Calendars
E-mail Newsletters
Linking to us
Links Disclaimer
Online Permission

e-business

Ridge: Link driver's license, visa

BY William Matthews
March 15, 2002

Printing? Use this version.
Email this to a friend.

The Office of Homeland Security is urging states to establish tighter control over foreign visitors by issuing driver's licenses that expire when visas expire.

"Driver's licenses get another look" [Federal Computer Week, Jan. 21, 2002]

The office is drafting model legislation to require that driver's licenses issued to non-citizens be tied to visas, homeland security spokesman Gordon Johndroe said March 14. The model is to be sent to the states for consideration by legislatures.

"ID card plan assailed" [Federal Computer Week, Feb. 18, 2002]

"System proposed to track foreigners" [FCW.com, Jan. 31, 2002]

In recent weeks, Tom Ridge, director of the Office of Homeland Security, has been encouraging governors and other state officials to take steps to improve the security and authenticity of driver's licenses.

In a conference call with state officials March 7, Ridge told state emergency management officials that he hopes motor vehicle departments can be electronically linked to databases maintained by the federal Immigration and Naturalization Service. That would enable state workers to check the immigration status of foreign nationals who apply for driver's licenses and issue licenses that would expire when visas expire.

Such capability also could enable the states to help keep better track of visiting foreigners.

INS has asked Congress for $380 million to build an entry and exit data system to keep track of foreign visitors. The system may include biometric identification information such as fingerprints or eye scans of visa holders. Such information also could be included on driver's licenses.

Ridge's telephone remarks came about 10 days after he urged governors attending a National Governors Association meeting to draft model legislation setting standards for more secure licensing procedures. By coming up with their own standards, Ridge said, the governors would avoid having standards forced on them by Congress.

Driver's licenses became a source of concern after the Sept. 11 terrorist attacks because most of the terrorists used such licenses --- obtained

Privacy Policy
Site Map
Subscriptions

Site Problems?

VENDOR SOLUTIONS
Vendor Directory

SCP
Cit-Pad
HP White Paper
NITAAC

legally and illegally — for identification.

The American Association of Motor Vehicle Administrators is pressing Congress to pass a law requiring states to adopt more uniform standards for driver's licenses and stricter procedures for issuing them.

AAMVA officials said they want licenses to include security features that make counterfeiting more difficult, and they want some form of "unique identifier," possibly a biometric identifier such as a fingerprint or eye scan.

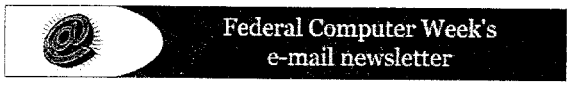
The AAMVA also wants much more thorough verification of a license applicant's identity before a license is issued. To accomplish that, the association wants Congress to earmark as much as $100 million for a computerized Driver Record Information Verification System that would enable federal and state agencies to more readily share information they have collected on drivers.

Thus, identification verification might involve cross-checking data submitted by license applicants with government databases that contain names, addresses, passport numbers and Social Security numbers, law enforcement records and INS data, AAMVA officials said.

The association also wants state driver's license databases to be interconnected so that licensing officials can check to see whether applicants already have licenses from other states.

Privacy advocates oppose high-tech licenses backed by interconnected databases, fearing driver's licenses will come to be used as national identification cards.

Johndroe said the model legislation the Office of Homeland Security is drafting "isn't intended to lead to a national ID card; it is intended to strengthen homeland security."



FCW.COM is a product of FCW Government Technology Group, a 101 Communications company

American Association of Motor Vehicle Administrators

Testimony of

Betty Serian
Vice Chair

American Association of
Motor Vehicle Administrators

A License to Break the Law?
Protecting the Integrity of Driver's Licenses

Submitted to the

Committee on Governmental Affairs

Subcommittee on Oversight of Government
Management, Restructuring and
the District of Columbia

U.S. Senate

Washington, DC

April 16, 2002

4301 Wilson Blvd, Suite 400 • Arlington, VA 22203 • Tel 703.522.4200 • Fax 703.522.1553
www.aamva.org

Good Morning Senator Durbin and distinguished Members of the Subcommittee on Oversight of Government Management, Restructuring and the District of Columbia. My name is Betty Serian and I am the Deputy Secretary for the Pennsylvania Department of Transportation and First Vice Chair of the Board of Directors for the American Association of Motor Vehicle Administrators (AAMVA). I also served as Chair of AAMVA's Identification Security Task Force. Thank you for the opportunity to appear before you today to speak about reforming the driver's licensing process and identification security.

AAMVA is a nonprofit voluntary association representing all motor vehicle agency administrators and chief law enforcement officials throughout the United States and Canada. AAMVA members administer the laws that govern motor vehicle operation, the driver credentialing process, and highway safety enforcement. DMV administrators are appointed by their state governors and their motor vehicle agencies receive funding from their respective state legislatures. AAMVA has played an integral role in the development, deployment, and monitoring of both the commercial driver's license (CDL) and motor carrier safety programs throughout the United States. The Association's members are responsible for administering these programs at the state level, and our members pride themselves on the work they do everyday to improve safety on our nation's highways.

As an international safety association, we have a responsibility and obligation to do our part to improve public safety and national security throughout North America. We believe this hearing will generate much needed public discourse about the critical public policy issue of reforming the driver licensing process and identification security.

Background

On September 13, 1899, Henry Bliss became the first traffic fatality in the United States. Mr. Bliss was knocked down and run over as he was stepping from a streetcar in New York City. The driver was arrested and held on $1000 bail. In 1902, only 23,000 cars were in operation in this country compared with 17 million horses. By 1932, growth in motor vehicles, increasing interstate travel, and the rising number of deaths and injuries on the highways created the need for a national organization for cooperative and uniform interstate consideration of laws and programs. In 1933, 23 states, the District of Columbia and some Canadian provinces formed what is today known as the American Association of Motor Vehicle Administrators. A congratulatory message from President Franklin D. Roosevelt stated "The North American Conference of Motor Vehicle Administrators offers a real opportunity for the cooperative solution of one of today's most perplexing problems."

In 1938, the first "Minimum Driver License Examination Standards" and "Standard Examination for Drivers" — the original basic standards for driver licensing — were created. AAMVA helped carry forward programs in driver licensing that resulted in all states having driver laws, in which every new applicant is tested on the basic elements of the standard driver's license examine. Since 1954, all states have required drivers to be licensed, and since 1959 all states have required examination prior to licensing. Over the last 50 years, AAMVA has developed programs to encourage uniformity, reciprocity, and sharing of best practices among the states and provinces, and liaisons with other levels of government and the private sector. Today with 228 million license drivers in the U.S. and Canada, AAMVA's program development and research activities provide guidelines for more effective public service.

The original purpose of the driver's license, first issued in 1903 in the state of New York, was to certify that an individual had earned the privilege to operate a motor vehicle. However, the driver's license has become much more than a license to drive. Over the last 40 years, the use of

the driver's license changed due to the demand for identification put on the public by the private sector.

Now, allow me to tell you three stories about a few Americans.

Larry and Rita Beller and Edward and Alice Ramaeker, four retirees, spent their golden years traveling across the country. Earlier this year, they were killed on a New Mexico highway by a repeat DWI offender. The driver, holding eight prior convictions from different states, was under the influence of alcohol and plowed head on into the retirees' car.

Emeke Moneme, an Ohio resident, had his wallet stolen from a local gym. Within weeks, Emeke discovered an identity thief had opened 13 fraudulent accounts in his name, totaling $30,000 in bad credit debt. It took him months to clear his name and straighten out his life.

Sara Clark, a schoolteacher and newly engaged, was killed after her flight was overtaken by terrorists and crashed into the Pentagon. Terrorists boarded the ill-fated flight using fraudulently obtained driver's license.

- Sara Clark shared her sad fate with more than 3,000 other Americans on 9/11.
- Larry and Rita Beller, and Edward and Alice Ramaeker, share the list of DWI fatalities with more than 16,000 Americans each year.
- And, Emeke Moneme shares victimization by identity theft with hundreds of thousands of Americans. Stealing someone's identity information, such as credit cards or Social Security Numbers, to take money or commit fraud is one of the fastest-growing crimes in the U.S. According to the Federal Trade Commission, 42% of the 204,000 complaints filed last year involved identity theft – resulting in billions of dollars of loss.

A common thread to these tragedies? The driver's license. In fact, the driver's license has become the most requested form of ID in the U.S. and Canada. For example, financial institutions require it to open an account, retail outlets ask for it when you want to pay by check, and the airlines demand it before you board a plane. In a recent (April 2002) poll conducted by Public Opinion Strategies, 83 percent of the American public noted that they used their driver's license for purposes other than driving.

The U.S. has more than 200 different, valid forms of driver's licenses and ID cards in circulation. In addition, each of the 50 states and D.C. have different practices for issuing licenses. Although the current system allows for reciprocity among the states, *it lacks uniformity*. Individuals looking to undermine the system, whether it is a terrorist, a drunk driver or an identity thief, shop around for licenses in those states that have become the weakest link.

In addition, the lack of standard security features on a driver's license allows individuals to exploit the system. While all states use a variety of security techniques, it is difficult for law enforcement and for those issuing a new license to verify the validity of a license from another state – not to mention the identity of the person holding the license. This situation is worsened by the availability of counterfeit driver's licenses and fraudulent breeder documents, such as a birth certificate or Social Security card, over the Internet and on the underground market.

AAMVA Efforts to Improve Uniformity for the Driver's License/ID Card

We at AAMVA commend you, Senator Durbin, for your focus on the need for a comprehensive reform of the driver's licensing process and identification security. In the days following September 11, Americans quickly learned how easily terrorists obtained a driver's license. All of the terrorists either legally or illegally obtained valid or bogus licenses and ID cards.[1] What is saddening, is that it took this catastrophic event to heighten America's awareness to the importance of ensuring the security of ID credentials — like the DMV-issued driver's license.

In October 2001, the AAMVA Executive Committee developed and passed a resolution establishing the Special Task Force on Identification Security. The Task Force was organized into five working groups focusing on technology, new issuance/initial identification, residency issues, document security/standards and communications/advocacy. The working groups produced reports that addressed the current situation and identified gaps, key issues, barriers, conclusions and results. The Task Force concluded that there were a number of common issues needing to be addressed: administrative processing, verification/information exchange, the need for a unique identifier, the format of the driver's license/ID card, fraud prevention and detection, residency, and enforcement and control of standards.

In January 2002, the Task Force, recommended eight broad strategies:

1. Improve and standardize initial driver's license and ID processes.
2. Standardize the definition of residency in all jurisdictions.
3. Establish uniform procedures for serving noncitizens.
4. Implement processes to produce a uniform, secure, and interoperable driver's license/ID card to uniquely identify an individual.
5. Establish methods for the prevention and detection of fraud and for auditing of the driver's license/ID processes.
6. Ensure greater enforcement priority and enhanced penalties for credential fraud.
7. Seek U.S. federal and other national requirements for legislation, rule making and funding in support of AAMVA's identification and security strategies.
8. Establish public and stakeholder awareness and support.

AAMVA has identified and targeted the areas that need improvement to reform the driver's license/identification process to achieve the recommendations from the Task Force. AAMVA and its members have been working to improve and unify the driver's licensing process for years. The association has several other projects dealing with the driver's license document and its issuance and support system:

Uniform Identification Practices Model Program

AAMVA developed a model administrative procedures program for issuing driver's licenses and ID cards. First published in 1996, AAMVA is currently revising this model program. Major topics of the model program are issuance procedures (initial, renewal and duplicates), unique identifiers, communication with federal agencies, name changes, maintenance of an acceptable identification document list, residency and legal presence, foreign documents, sanctions, security features, and technology. We continue to work toward further harmonization among the states by encouraging the use of the model program. The Uniform Identification Practices Model Program is one of the most popular programs adopted by the states that AAMVA has developed.

---

[1] See FBI List of Terrorists.

Fraud Prevention Programs

The use of fraudulent documents has caused enormous economic losses in both the U.S. and Canada. In the early 1990s, in conjunction with NHTSA and the Florida Division of Motor Vehicles, AAMVA, under contract with West Virginia University, developed and implemented a training program including model training materials for the Fraudulent Identification Prevention Program (FIPP). A revision of FIPP training materials was then completed in April 1996. Most recently, the use of fraudulent documents has become a national security issue for both countries as well as foreign countries. The use of fraudulently obtained identification is also directly related to losses in human life on our highways. The use of fraudulent documents to obtain driver's licenses/identification cards has grown exponentially in recent years. Services for obtaining fraudulent documents are easily available through the Internet and other means. In addition, fraudulent breeder documents (Passports, Visas, Social Security Cards, birth certificates, INS Documents, driver's licenses or Identification Cards), which are commonly forged, altered or counterfeited are commonly used to obtain valid driver licenses.

For years AAMVA has provided Fraudulent Document Recognition Train-the-Trainer courses throughout the U.S. and Canada. AAMVA has educated hundreds of fraud recognition trainers for state and provincial motor vehicle agencies. AAMVA has recognized the need to revise existing training materials as well as the need to establish a more comprehensive national model-training program for state and provincial driver licensing personnel and law enforcement officials for the recognition of fraudulent documents. We are updating this course in cooperation with various federal agencies. However, interim training will continue during this revision. AAMVA is creating a "best practices" document that will provide an overview of how state and provincial motor vehicle and law enforcement agencies deal with these issues.

Driver's License/ID Document Standard

AAMVA is involved in creating a driver's license document standard, both nationally and internationally. Work began in 1996. National and international standards ensure that documents are interoperable among the issuing jurisdictions — the bar code on an Iowa license may be read by a trooper in New York and vice versa. On a national level, AAMVA has developed and published the AAMVA Driver's License/ID Card Standard that is being used by some states for creating a driver's license and ID card. AAMVA is in the process of further improving this standard and working with more states to ensure that they adhere to its provisions when they create a new document. We continue to work toward further harmonization among the states in using the standard.

Foreign Reciprocity

AAMVA finalized a foreign reciprocity resource guide for its membership in October 2001. This was a major undertaking by AAMVA to compile information on foreign driver's license documents, practices and procedures that will enable our members to make more informed decisions on entering into bilateral agreements with foreign countries. One of the key issues was how to deal with foreign driver's license assessment and verification of the person's license. Topics contained in the resource guide are Legal Considerations; Model and Existing Driver's license Reciprocity Agreements; Issues to Consider before entering into a Reciprocity Agreement; Model and Existing Enabling Legislation; Driver Licensing Standards; and Foreign Driver's license Assessment and Verification of Driver Status.

Drivers License Agreement (DLA)

The Driver License Joint Compact Executive Board (the Board) began work on the Driver License Agreement (DLA) at the Compact Annual Membership meeting in October 1996. Having originated in concept with the 1994 establishment of a North American Driver License

Agreement (NADLA) task force, the DLA emerged to become the Board's main focus. The Board gathered input that would unify the existing Driver License Compact (DLC) and the Non-Resident Violator Compact (NRVC).

A 1994 Compact Compliance Survey of members indicated that no member jurisdiction was in full compliance with either Compact. The results of a 1997 survey of members established the primary components of the DLA.

The DLA is a voluntary, reciprocal agreement among member jurisdictions to promote the "one license-one driver control record" concept and to provide for the fair and impartial treatment of all drivers operating within their respective borders. The DLA deals specifically with the issuance and retention of driver's licenses, the update and maintenance of driver records, compliance with the laws and regulations relating to highway safety and federal mandates, as well as the exchange of information between member jurisdictions. In the effort to truly establish a one driver, one record system, the new DLA will be a more efficient and effective agreement for the jurisdictions to share and transmit driver and conviction information.

The DLA is vital in creating and maintaining a traffic safety program that should begin with a Uniform DL/ID Security System. Upon issuance of the driver license, the DLA would provide specificity regarding the retention of the license, the update and maintenance of driver records, compliance with the laws and regulations relating to highway safety and federal mandates, as well as the exchange of information between member jurisdictions. The DLA would ensure that the integrity of the process achieved at the time of issuance is maintained during the life of the document. The DLA was approved by the AAMVA membership in the fall of 2000.

Information Systems

AAMVA has been investigating, implementing and operating information systems on behalf of its members since the late 1980s. Through its technology subsidiary, AAMVAnet, AAMVA manages and operates the Commercial Driver's License Information System (CDLIS), which is designed as a clearinghouse for commercial drivers. CDLIS was designed to limit any given commercial driver to **one and only one** commercial driver's license and it has worked well for this purpose. AAMVAnet also supports the National Driver Register/Problem Driver Pointer System (NDR/PDPS) owned by NHTSA. PDPS is used to determine whether or not a given driver's license applicant is or has been under license withdrawal anywhere in the U.S.

In the mid-1990s, AAMVA began exploring the possibility of having a clearinghouse of all drivers within the U.S. in order to better control the problem driver population. States need more effective tools to manage the driving records *we already maintain.* Problem drivers, who obtain multiple licenses, spread their bad driving history across the states. As a result, they avoid detection, penalties and punishment. By 1999, Congress recognized the potential benefits of such an information system and directed NHTSA to study the IT issues and costs associated with developing and operating this clearinghouse. Immediately, NHTSA tapped AAMVA to do this assessment. The report concluded that an all-driver system is feasible.

We need a system, such as the proposed Driver Record Information Verification System (or DRIVerS), to keep bad drivers off the road and save the lives of those whom responsibly use the privilege to drive. DRIVerS is a pointer system that allows the DMV in one state to query the driver records in another state and to accurately verify driving history of the appropriate person.

DMVs already exchange driver history on commercial vehicle drivers through the 1986 federally mandated CDLIS. Since CDLIS was implemented, there have been no privacy concerns. And

within a four-year period alone, CDLIS has kept 871,000 potentially dangerous commercial vehicle drivers off the roads.

Need for Federal Partnership

AAMVA programs have been successful in varying degrees over the years. AAMVA is not a regulatory body and its members operate under self-regulations. Relying on self-regulation is difficult and prevents the states from achieving 100 percent uniformity in the driver's licensing community. Without 100 percent participation from the states, the driver's license system is only as strong as the weakest link — that is why we need federal partnership.

The need for federal partnership is highlighted by the success we have had with the Commercial Driver License (CDL) program and the failure we have had with the Driver License Compact. The CDL Program is a federal/state partnership that was fully functional in all states within six years of the passage of legislation. The Driver License Compact has been in existence for over 40 years. Even today, not all states are members of the compact and based on a survey that we conducted in 1994, no state fully complies with the tenants of it.

Since the events of September 11, the need for a federal-state partnership is even stronger. In fact, AAMVA has found over 20 states have introduced some form of legislation that strengthens driver's license procedures. Unfortunately, this piecemeal approach only begets more lack of uniformity. Some of the obstacles that states face in attempting to implement more secure measures are budget constraints, lack of funding for initiatives, and state legislatures not passing legislation for years. In order to get the full participation of every state, we need the federal government to create a partnership with the states to improve the driver's license/identification process. Without federal involvement, it will take the system many years to change. We think time is of the essence.

Conclusion

The American public wants a more secure license. **Seventy-seven percent (77%) of the American public support** Congress passing legislation to modify the driver's licensing process and identification security. And, we need Congress to help in five areas:

1. Support minimum compliance standards and requirements that each state must adopt when issuing a license.
2. Help us identify fraudulent documents.
3. Support an interstate network for confirming a person's driving history.
4. Impose stiffer penalties on those committing fraudulent acts.
5. And, provide funding to make this happen. Funding so states can help ensure a safer America.

Our goal is **one driver, one license and one driving history**. The American people expect Congress to reduce the number of people being victimized by dangerous drivers and identity theft. Most importantly, the American people expect you to do what you can to save lives — to prevent deaths of people like Larry and Rita Beller, Edward and Alice Ramaeker, Sarah Clark and thousands of other Americans. When we can verify identity, we're one step closer to preventing fraud, protecting privacy, and saving lives.

AAMVA stands ready to assist the Committee in developing legislation to improve driver's licensing process and identification security.

Thank you. I've concluded my testimony and welcome any questions from the subcommittee.

If you or your staff have any questions about our testimony, please do not hesitate to contact Tom Wolfsohn, AAMVA's Senior Vice President of Government Affairs and Communications at (703) 522-5791.

Mohamed Atta
FL DL, 05/02/2001

Khalid Al-Mihdhar
CA DL, 04/05/2000
USA ID card*, 07/10/2001
VA ID card**, 08/01/2001

Hani Hanjour
AZ DL, 11/29/1991
FL ID card, 04/15/1996
VA ID card, 08/01/2001
Failed VA DL test, 08/02/2001
MD ID card, 09/05/2001

Satam Al-Suqami
No DL or ID card

Ahmed Al-Ghamdi
USA ID card, 07/2001
VA ID card, 08/02/2001

Hamza Al-Ghamdi
FL ID card, 06/26/2001
FL DL, 07/02/2001
(duplicate issued 08/27/2001)

Ahmed Al-Nami
FL DL, date of issue unknown

Ahmed Al-Haznawi
FL DL, 07/10/2001
(duplicate issued 09/07/2001)

Saeed Al-Ghamdi
FL DL, 07/10/2001

Abdul Al-Omari
USA ID card, 07/10/2001
VA ID card, 08/02/2001

Marwan Al-Shehhi
FL DL, 04/12/2001

Nawaf Al-Hazmi
CA DL, 04/05/2000
FL DL, 04/25/2001
USA ID card, 07/10/2001
VA ID card, 08/02/2001

Ziad Jarrah
FL DL, 05/02/2001
VA ID card, 08/29/2001

Waleed Al-Shehri
FL DL, 05/04/2001
(duplicate issued with different address, 05/05/2001)

Majed Moqed
USA ID card, 07/2001
VA ID card, 08/02/2001

Mohand Al-Shehri
FL ID card, 07/02/2001

Wail Al-Shehri
FL DL, 07/03/2001

Fayez Banihammad
FL ID, 07/10/2001

Salem Al-Hazmi
USA ID card, 07/2001
VA ID card, 08/02/2001

ams

Testimony of

Barry J. Goleman

Vice President, Public Sector

American Management Systems, Inc.

United States Senate

Committee on Governmental Affairs

Subcommittee on Oversight of Government Management, Restructuring and the District of Columbia

"A License to Break the Law? Protecting the Integrity of Driver's Licenses"

April 12, 2002

I would like to thank Chairman Durbin, the Ranking Member, and the other members of this committee for the opportunity to appear here today.

I am a vice president in the Public Sector Group at American Management Systems. AMS is a business and information technology consulting firm with international headquarters located in Fairfax, Virginia. In 2001, AMS had revenues of $1.18 billion. We employ more than 7,000 people in 51 offices worldwide. Our business is equally split between the public and private sector, with about one-half of our public sector work serving state and local governments. Our clients have included more than 90 percent of U.S. federal civilian agencies, all U.S. military and major defense agencies, 41 U.S. state governments, and eight of the top 10 U.S. cities.

AMS specializes in the intelligent application of information technology. Our size and balanced business portfolio give us the agility to work across the public and private sector, introducing innovative solutions and best practices across industries and government.

I have been involved in the issuance of driver's licenses, and the information systems to support that process, for more than 29 years—first as a driver's license examiner for the State of California and later as the president of the American Association of Motor Vehicle Administrators (AAMVA) information technology subsidiary, AAMVAnet. In my capacity as an examiner, I was presented with counterfeit documents to obtain a license, I stopped people from stealing identities for the purpose of cashing stolen checks, and I was offered bribes to issue false identification. I come here today in support of your efforts to strengthen the integrity of the driver's license because I know what work needs to be done, and I know that this work can be done—if state and federal agencies and the technology industry will work together to make it happen.

Senator Durbin, I commend your committee for its thoughtful approach to this challenging task. It is obvious, especially in the wake of our nation's new homeland security imperative, that the problems of identity theft and fraud must be addressed quickly. Prior to September 11, driver's license fraud and identity theft often were viewed as financial crimes or teenage pranks. According to research conducted by the Yankee Group, during the year 2000, the Financial Crimes Division of the Secret Service made 10,000 arrests involving identity theft or fraud. Such crimes can have as many as 750,000 victims and cost consumers tens of millions of dollars annually. As you know, the investigation subsequent to September 11 has placed the problems of identity theft in a whole new light. We learned that terrorists, bent on destroying the American way of life, used our state motor vehicle agencies to create identities that allowed them entry into our economic and transportation systems. They were able to accomplish this because the driver's license, or state-issued identification card, is the de facto identification used by Americans to prove their identity within our borders.

This recognition of the driver's license as a trusted form of identification has grown out of its use in everyday American life: retailers use it for check cashing, banks for account verification, and airports for security access. One of my own encounters with how much trust is placed in the driver's license occurred when I was required to present documents proving my American citizenship to be employed by a federal agency. I provided my naturalization papers, as I was born

outside the United States to American parents. Instead of using my secure naturalization papers to verify my identity, the personnel clerk asked to see my driver's license. You may remember that 6 of the 19 hijackers on September 11 used stolen identities. The terrorists obtained multiple IDs because they knew that the driver's license was a trusted form of identification, and these terrorists were able to leverage the weaknesses in our state identification systems with devastating consequences. Therefore, it is imperative that we improve the integrity of the driver's license so that it can live up to its reputation as a trusted personal identification document.

To address this critical homeland security threat, state and federal agencies should develop a strategy that takes advantage of rapid evolution. By that, I mean adapting and expanding existing technology, relatively quickly, and capitalizing on existing infrastructure. We do not need to reinvent the wheel here. Existing state-based assets can be used to create a more secure identification to combat the problem of identity fraud and theft.

Some have called for a new national identification system, built essentially from scratch, but this proposed solution is neither feasible nor quick to implement. States already have an extensive, functioning infrastructure through their motor vehicle agencies. It is essential to capitalize on the existing information assets maintained by these state agencies.

Identification fraud, also known as identity theft, is exacerbated by the 50 states issuing a confusing array of state licenses that use a range of security features and rely on easily forged or counterfeit documents. Law enforcement experts estimate that there are more than 240 valid driver's license formats in circulation. As we have seen, identity theft is a security breach with enormous consequences. New state-issued and controlled secure personal ID cards, based on national standards, are an essential component of maintaining our nation's security. To issue personal identification documents that ensure the highest level of security, national standards should be developed around the following processes:

- Verification of source documents prior to their acceptance as proof of identification
- Issuance of a new, secure, tamperproof driver's license or other personal ID document
- Authentication of the ID with visual and machine-readable features

The most persuasive argument for turning to state motor vehicle agencies for improved personal ID verification processes is that these agencies are already in the identification business. This enormous, functioning infrastructure can be adapted by providing national standards and enhanced technologies to verify identification and detect fraud.

Many proponents of a secure personal ID system will tell you about the value of biometrics and smart-card technologies, and clearly these technologies can provide substantial benefit. To provide maximum security, these next-generation ID documents must adhere to standard security features using the highest level of tamper-resistant technologies available. Biometrics, for example, can complete a positive one-to-one authentication of the person to the card. In addition, smart cards can make the driver's license a carrier for important data such as including the biometric identifier right on the card itself or other optional data that individuals may wish to add, such as emergency medical information or digital government access.

These new technologies are an important part of our future, but if they are used without improved verification technologies, they will be useless as secure, reliable forms of identification. As you draft new legislation to improve the integrity of the driver's license, I urge you to consider new technologies that can be used to verify identity. This will ensure that people with counterfeit or false IDs won't receive better, more secure ID documents.

The first step in securing identification is a thorough verification of the individual's identity before enrolling them in the system. To accomplish this verification, state examiners must have access to the data backing up these documents, such as birth records and immigration data. Databases are more difficult to falsify than paper documents

The second step is addressing privacy concerns by ensuring that the data is verified but not copied or aggregated into a consolidated personal identification database. Today's Web services technologies can exchange data between these databases and secure personal data from unintended disclosure. The simple fact is that if you don't do a better job of establishing an individual's identity before you issue a new, secure driver's license, you will not have achieved your goal of making the driver's license a more trustworthy document.

For example, technology is available to assist driver's license examiners make better identification decisions. These tools can be used to verify data from the driver's license application (name, address, Social Security number, etc.) by leveraging existing public consumer databases. The examiner can quickly check and confirm the applicant's information, validate the identity, and identify fraudulent information during the driver's license transaction. Discrepancies can be resolved by requesting additional documentation from the applicant or, in some cases, no license will be issued until further checks are made at the central office. States and federal governments are in the process of testing solutions like this in an effort to improve the basis for making identification decisions.

The third step in developing a secure ID system is the prevention or deterrence of employee fraud. Just as I was occasionally offered bribes of cash or sexual favors in exchange for issuing driver's licenses, today's examiners have their integrity challenged when criminals seek any path to obtain a valid state license. (For the record, let me assure you that I refused these attempted bribes.) Unfortunately some have not resisted these kinds of temptations, and the resulting scandal and corruption are well documented. Effective employee fraud deterrence by a responsible licensing administrator must include internal auditing and business intelligence tools.

There is tremendous power and sophistication in software already in use in the commercial sector. This technology underlies millions of everyday transactions in the marketplace and enables a more rigorous approach to auditing and decision support. These same tools can be used to monitor driver's license transactions and highlight behaviors and patterns that warrant further investigation. For example, it takes about 45 minutes to complete a commercial driver's license test administered according to Federal Motor Carrier Safety Administration rules. As a supervisor, I would want to investigate an examiner that issued commercial licenses in 10 minutes. Sadly, today many state motor vehicle agencies are unaware of these fraudulent activities until agency co-workers or the public report suspected activity. This is an example of the application of proven technology from the business sector.

All of these steps are achievable with federal, state and private-sector cooperation. From my experience working with state and federal agencies to improve motor vehicle systems, I can assure you that the application of best practices in the state issuance process—supported by robust and effective information technology—can result in a secure and trustworthy means of personal identification.

The IT industry uses sophisticated technology and management know-how to open doors to better efficiency, productivity, and prosperity however, we must be willing to work in a public-private partnership to close doors that will keep out those who want obtain false identification and move freely about our commercial, financial, and transportation systems.

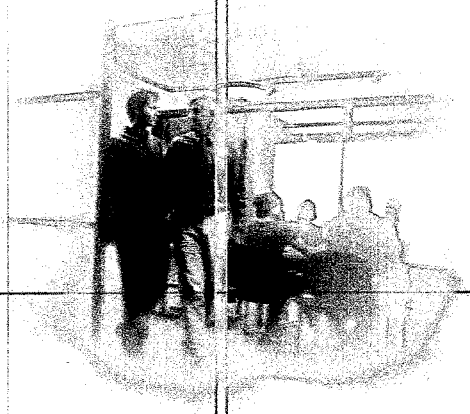
I am sad to say that, in the aftermath of September 11, we've learned that the terrorists obtained multiple driver's licenses and ID cards from state motor vehicle agencies with ease—some using fraudulent documents or bribes. Despite this breach in security, there is encouraging news: this is a problem that we can fix. With technology that exists today, we can stop the fraud and counterfeiting of state licenses. The states and federal government worked cooperatively from 1987 to 1992 to implement the requirements of the Commercial Motor Vehicle Safety Act. Federal grants were made available to states to implement new strict standards that were developed in cooperation with state licensing experts. That cooperative effort serves as an example of how to solve problems by employing technology and leveraging the combined strengths of federal and state agencies. Working together, again, we can solve this homeland security problem.

Senator Durbin, we at AMS believe that this committee is on exactly the right track by holding this hearing and advocating the development of a more secure driver's license. We believe technology can advance identification security while preserving our personal freedoms.

Thank you. I look forward to your questions.

Attachment: AMS White Paper, "Establishing a National System for State-Issued Secure Personal Identification"

Establishing a National System for State-Issued Secure Personal Identification



Barry Goleman, vice president, AMS

November 2001

AMS Proprietary and Confidential

"Our membership, as the de facto issuers of identity documents in the United States, has long recognized the problems caused by fraudulent identification documents and has been working to improve their detection and prevention. The recent terrorist attacks on American soil were perpetrated by those that used false identification to position themselves to strike at our nation. These events have only hardened our resolve to find effective ways of dealing with this problem."

American Association of Motor Vehicle Administrators (AAMVA) September 20, 2001

Overview

Over the course of the past 50 years, the ability of individuals in the United States to identify themselves, to prove that they are who they say they are, has depended primarily on the state issued driver's license. The eventual adoption of photo licenses by all states further reinforced our national reliance on the driver's license as an identification card.

However, as the motor vehicle agencies themselves have acknowledged, our de facto system of identification is flawed. These state agencies own the identity program more through a progression of photo license technologies than through a specific public policy decision to assign responsibility and resources in these agencies. As public policy makers search for solutions to ensure secure identification, improving the identification practices of the state motor vehicle agencies must be a primary objective.

Identification fraud or identity theft is facilitated by the fact that 50 states issue a confusing array of state licenses using a variety of security features and relying on easily forged or counterfeit documents. Once considered primarily an economic crime or juvenile pastime, identity crime is now recognized as a security breach that may have enormous consequences for our nation. The terrorist attacks on September 11th highlight the need for secure identification as a preventative measure to facilitate the security of our nation's transportation network.

New licenses or identification cards based on national standards are an essential component of protecting our Homeland Security. The identification document will rest on three pillars of national standards to ensure security:

- **Verification** of source documents prior to accepting them as proof of identification,
- **Issuance** of a new secure, tamperproof driver/ID document, and
- **Authentication** of the license with visual and machine-readable features.

National Standards

National standards are the key to a new identification program. At present, state driver's license characteristics (size, durability, security features) grew out of credit card industry practices and are largely determined by the vendor community. Depending on the state's past and current vendors and the longevity of license periods, a state may have two or three driver's license formats in circulation at any one time. Law enforcement experts estimate there are over 240 valid driver's license formats in circulation today, making knowledgeable visual authentication based on license characteristics an

impossible task to the average person presented with an ID. Of equal importance is the need for new national standards to verify supporting identification documents and for technical standards for exchanging identification data.

In the federal-state governance model, numerous examples exist of motor vehicle agencies implementing federal standards. This cooperative relationship leverages the best aspects of the federal government's regulatory process to create uniformity and the state capability to deliver service at the local level.

The Role of the States

There has been much recent discussion calling for a new National Identification Card, which would essentially duplicate the state issued driver's license. The most persuasive argument for turning to motor vehicle agencies for identification is that they are already in the identification business. Motor vehicle administrators know the strengths and weaknesses of the current system and they have a compelling public policy reason to provide a new solution. These agencies control the state's largest database of personal information and they have existing interstate messaging standards (though their network, AAMVAnet) that can be expanded to include new sources for verification. The state infrastructure of branch offices provides a localized resource to reach more citizens than any other state agency. To issue a National Identification Card, this localized delivery system would have to be needlessly duplicated.

Although the public's perception of government inefficiency and the state Department of Motor Vehicles (DMV) is often shaped while standing in seemingly never-moving lines, in fact the state motor vehicle agency is part of a sophisticated data communications network. State DMV's currently exchange data on commercial drivers through the Commercial Driver License Information System (CDLIS), suspended and revoked drivers through the Problem Driver Pointer System (PDPS), and vehicle titles through the National Motor Vehicle Title Information System (NMVTIS). Expansion of these capabilities to include information about all drivers and authentication data such as biometrics could be accomplished through the already-conceived Driver Record Information Verification System (DRIVerS). DRIVerS is to be an on-line system that gives licensing officials the ability to instantly verify out-of-state driver license information when a driver moves from one state to another.

The state-federal relationship can also be used to further secure identification objectives. Through the American Association of Motor Vehicle Administrators (AAMVA), state motor vehicle agencies have an existing commitment with the U.S. Departments of Transportation (DOT) and Justice (DOJ) to implement national standards for licensing and vehicle information. This cooperative relationship has grown steadily since the 1986 enactment of the Commercial Motor Vehicle Safety Act and the creation of the CDLIS as a means to ensure that a commercial driver will only have one license and that all enforcement actions will be carried on a driver's single record. As originally envisioned by Congress, this would have been a federally issued license—but DOT worked with the states and the AAMVA to change state licensing programs to comply with new federal statutes and regulations. This cooperative model was facilitated by the distribution of grant funds to support state initiatives. This same model of cooperation and funding is needed to implement a national ID standard and support state computer upgrades and training.

The Three Pillars of a National ID Standard

Verify Source Documents

One of the most effective ways to commit identity fraud is to thwart the controls of an identification system by falsely obtaining a valid license from the issuing agency. A common path for obtaining a false license is to present counterfeit or forged documents as verification of identity. The combination of scanners, laser printers and high quality mail order paper enable the home production of official-looking birth certificates and other documents with minimal investment.

Verifying residency or immigration status is one of the most daunting tasks facing many state DMV's. The financial industry has already confronted this problem and has developed sophisticated tools to enable verification of address and other personal data for processing on-line and telephone credit applications. Credit bureaus and other non-governmental databases have substantial address information and records of identity fraud in financial transactions. These data sources are not currently being used by states to substantiate the identity information offered by individuals. At a minimum, these same tools should be adopted by states for fraud investigation and/or to verify questionable documents.

In a secure identification program, source documents (often referred to as "breeder" documents) are not accepted at face value but are verified against their original source. Numerous state and federal databases contain identifying data that can be cross-referenced and matched to close the system to people with forged documents. Some useful databases include:

- SSN verification
- Passport and INS data
- Birth and death Vital Statistics
- Tax records
- Wage files submitted by employers
- Criminal history files
- USPS address file
- Commercial databases

Another key element of verification is communication between states when drivers relocate. When a person relocates from one state to another, the driver license data could be obtained from the prior state to verify the license by contacting DRIVerS for state-to-state exchange of driver information.

To make a verification system possible, federal and state governments need to work cooperatively to make databases available for instant verification and publish standards by which states will send and receive messages to inter- and intra-state identification databases. Until now, connecting these islands of data was hampered by technical means and the lack of a bureaucratic imperative. Today's middleware solutions and Enterprise Application Integration (EAI) technology enable this type of data sharing on a broader scale without requiring internal changes to the existing legacy systems.

Issue Secure ID Documents

The second pillar supporting secure identification is the issuance of a new type of license containing high security features that should be standardized in federal regulations. These regulations must acknowledge the state issued driver's license/ID card as the 'government issued' identification required for U.S. residents and must delineate issuance standards and document security features. And by adopting these federal regulations into state law or regulation, states will acknowledge their identification mission.

Many states issue driver's licenses "over the counter" as a customer service. A similar instant issuance might continue to be available if all verification steps establish proof of identity, but states will need to adopt alternative procedures for delayed issuance of permanent licenses when further verification is needed or source data is not available. For example, until Immigration and Naturalization (INS) files are available on-line, a person using a non-resident alien card as a source may need to be issued a temporary non-certified license until an off-line search of INS files can be verified.

While it is important to critically evaluate competing opinions of security features such as holograms and security overlays to be incorporated into a national standard, a focused decision-making process will be necessary to select from the various technologies and move quickly to an implementation phase. New secure licenses will need standard embedded features that prevent forgery or counterfeiting and overcome the ability of copiers or scanners to reproduce the license data and substitute a different photo image. Government agencies and private industry have already compiled much of the research upon which to base these decisions.

Authenticate the ID Card

The third, and sometimes overlooked, pillar supporting a secure identification standard is the application of a simple, quick means to authenticate identification. The authenticator must be able to determine that the license is a valid identification issued according to the established standards and that the person presenting the license is the same person to whom it was issued. Today, someone checking a license must be able to make an authentication decision based his or her ability to match the photo or signature to the person presenting the card. Secure ID cards must include high security and biometric features designed to be instantly recognizable as valid and to prove that the person presenting the card is the same person originally issued the document.

To facilitate quick authentication the federal standards for licenses must define a standard format and data for state driver's licenses. The license should have one national standard size, color and layout with a single reserved area for a state logo or seal. Regulations must mandate holographic and other easily recognizable security features capable of being verified optically and by machine-readable technologies. The secure ID may include these features:

- Metalized holograms
- 2D Barcodes
- Smart card chips
- Embedded biometric templates

National ID Policy Issues

Privacy

The federal Driver Privacy Protection Act (DPPA) and additional state statutory and regulatory provisions protect the personal data contained in driver records today. Under a secure identification program states will need to access additional data sources to perform verification of identity that could raise new concerns about privacy and government records. Strong protection measures must be included as an integral part of the secure identification program and to ensure the privacy of personal information.

Biometrics

Any proposed new identification system should include biometric identification capabilities. Current research has questioned the ability of today's biometric technologies as a tool to prevent multiple enrollments into an identification system; however, limited uses such as authentication are feasible today.

Biometric techniques are used in two basic configurations. The first is enrollment, in which an individual is attempting to be entered for the first time and the issuer is trying to determine if that person is already in the database. This one-to-many search can create both false positives (a match is returned showing the individual is already enrolled when he is in fact a new unique identity) and false negatives (the person has been previously enrolled using a different identity but no match is made). The various biometric technologies each have their own error rates but, generally speaking, error rates and ease of use problems have prevented current biometric technologies from being adopted for enrolling a mass audience such as in the driver license issuance environment.

In the second configuration a one-to-one match can be used to authenticate that a person is the same person who was previously enrolled in the database. In these cases, a number of the current biometric technologies can perform an accurate match on the biometric data and authenticate the person's identity.

Available biometrics for authentication may include one or more of the following:

- Thumb print
- Finger or hand geometry
- Facial recognition
- Retinal or iris scan

Employee Fraud

The potential for employee fraud exists in any organization and, although rare, it is a constant threat in a motor vehicle licensing environment. Almost everyone who has worked in the identification or driver system has, at some point, been approached or questioned about the ability to falsify records or documents. As a deterrent to the few employees who actually succumb to financial or personal pressures to commit fraud, careful attention must be placed on audit and control.

A secure ID program must employ an internal audit system designed to prevent employee fraud and error through personnel oversight and procedural controls. The program must also apply audit standards and business intelligence tools to detect problems in issuance activity.

Summary

The public's need for secure identification has never been greater and the mission of the state and federal governments to address the shortcomings of the current system has never been more clear. The time to strengthen the identification system with new national standards is now. The states and their federal partners will face enormous challenges moving to this new secure identification system but the will and the capability exist to achieve dramatic improvements over the current system. Efforts are already underway with AAMVA, the states and their industry partners to take immediate action on a framework for securing the identification program.

The staff of AMS has extensive subject matter expertise in the business process and technologies of identification and is actively working with AAMVA, the member states and the federal government to support an identification program that will increase our nation's security.

References

"Buying a Brand-new Identity, " *Dateline NB,* 26 October 2001. http://www.msnbc.com/news/647826.asp

"Fake IDs Swamp Police," *USA Today,* 2 July 2001.

"September 11 and the Virginia DMV," *National Public Radio All* Things *Considered,* 18 October 2001. http://search.npr.org/cf/cmn/cmnpd01fm.cfm?PrgDate=10/18/2001&PrgID=2

Biometrics In Human Services: User Group Newsletter. www.dss.state.ct.us/digital.htm

FTC Clearinghouse on Identity Theft http://www.consumer.gov/idtheft/

International Association of Financial Crime Investigators http://www.iafci.org/start.html

National Biometric Test Center Collected Works, 1997-2000, edited by James L. Wayman. Version 1.3 Prepared under DoD Contract MDA904-97-C-03 and FAA Award DTFA0300P10092. August 2000. http://www.dodcounterdrug.com/facialrecognition/FRVT2000/documents.htm

Real Time Identity Authentication http://www.insideouttech.com

ams

About AMS

AMS is an international business and information technology consulting firm with 2000 revenues of $1.28 billion. Founded in 1970, AMS leverages cross-industry expertise to manage mission-critical IT, e-business, and systems integration projects for clients including 43 state and provincial governments, most federal agencies, and hundreds of companies in the *Fortune 500*. AMS's core strength is its deep pool of talented consultants with expertise in systems development and implementation, large-scale technology integration, change management, and e-business reinvention. AMS is headquartered in Fairfax, Virginia and has nearly 8,000 employees in 51 offices around the world. *Forbes* Magazine ranked AMS among "America's 400 Best Big Companies" and *Fortune* placed AMS 44th on its list of the "100 Best Companies to Work for in America." AMS is traded in the NASDAQ under the symbol AMSY and is on the Web at ams.com.

Contact Information

Barry Goleman
Vice President
AMS
State and Local Solutions
1215 K Street, Suite 1000
Sacramento, CA 95814
Phone: 916-283-2022
Mobile: 916-802-5987
FAX: 916-830-1199
Email: barry_goleman@ams.com

Statement by J. Bradley Jansen,

Free Congress Foundation
A License to Break the Law?

"Protecting the Integrity of Driver's Licenses" hearing
Senate Subcommittee on Oversight of Government Management, Restructuring and the District of Columbia

Committee on Government Affairs
April 16, 2002

Chairman Durbin, Senator Voinovich, members of the Subcommittee, thank you for allowing me the opportunity to present testimony on the subject of improving our identification practices. My name is Brad Jansen. I am the Deputy Director of the Center for Technology Policy at the Free Congress Foundation, a Washington, DC based think-tank focusing on the culture of American conservatism and our Constitutional liberties.

While the federal government has an important role to play in enhancing the security and reliability of the driver's license system, it is important that efforts to improve that system do not overstep the proper role of the federal government concerning the rights of the states and that such efforts do not unintentionally reduce the reliability and security of the driver's license system.[1]

The Free Congress Foundation, along with Eagle Forum, the Electronic Privacy Information Center and the American Civil Liberties Union, head a large, broad-based and informal coalition of groups opposing the introduction of a National ID. The American Association of Motor Vehicle Administrators (AAMVA) proposes to set uniform standards for driver's licenses for all states and to link the state driver's license databases.[2] The AAMVA protests that they do not consider their proposal to be a national ID. Their argument fails the "duck test": it looks like a national ID, walks like a national ID and quacks like a national ID.[3]

---

[1] See "National ID Threatens Freedom of Law Abiding Citizens," Free Congress Foundation, February 11, 2002. http://www.freecongress.org.

[2] AAMVA Executive Committee Resolution establishing the Special Task Force on Identification Security, October 24, 2001, http://www.aamva.org/Documents/hmExecResolution.pdf. and AAMVA Special Task Force on Identification Security Report to the AAMVA Board, Executive Summary, http://wwwaamva.org/drivers/drvIDSecurityExecutiveSummary.asp.

[3] See also "Your Papers, Please: From the State Drivers License to a National Identification System," Electronic Privacy Information Center, February 2002. http://www.epic.org.

Our ad hoc coalition made the following arguments in a letter[4] to President Bush urging him to reject the American Association of Motor Vehicle Administrators (AAMVA) proposal that the federal government would fund and authorize a proposal to standardize state drivers' licenses because:

A national ID would not prevent terrorism. An identity card is only as good as the information that establishes identity in the first place. Terrorists and criminals will continue to be able to obtain -- by legal and illegal means -- the documents needed to get a government ID, such as birth certificates and social security numbers. A national ID would create a false sense of security because it would enable individuals with an ID -- who may in fact be terrorists -- to avoid heightened security measures.

A national ID would depend on a massive bureaucracy that would limit our basic freedoms. A national ID system would depend on both the issuance of an ID card and the integration of huge amounts of personal information included in state and federal government databases. One employee mistake, an underlying database error rate, or common fraud could take away an individual's ability to move freely from place to place or even make them unemployable until the government fixed their "file." Anyone who has attempted to fix errors in their credit report can imagine the difficulty of causing an over-extended government agency such as the department of motor vehicles to correct a mistake that precludes a person from getting a valid ID.

A national ID would be expensive and direct resources away from other more effective counter-terrorism measures. The costs of a national ID system have been estimated at as much as $9 billion. Even more troubling, a national ID system mandated through state agencies would burden states who may have more effective ways to fight terrorism and strengthen ID systems.

A national ID would both contribute to identity fraud and make it more difficult to remedy. Americans have consistently rejected the idea of a national ID and limited the uses of data collected by the government. In the 1970s, both the Nixon and Carter Administrations rejected the use of social security numbers as a uniform identifier because of privacy concerns. A national ID would be "one stop shopping" for perpetrators of identity theft who usually use social security numbers and birth certificates for false IDs (not drivers' licenses). Even with a biometric identifier, such as a fingerprint, on each and every ID, there is no guarantee that individuals won't be identified - or misidentified - in error. The accuracy of biometric technology varies depending on the type and implementation. And, it would be even more difficult to remedy identity fraud

[4] See http://www.aclu.org/congress/l021102a.html.

when a thief has a National ID card with your name on it, but his biometric identifier.

A national ID could require all Americans to carry an internal passport at all times, compromising our privacy, limiting our freedom, and exposing us to unfair discrimination based on national origin or religion. Once government databases are integrated through a uniform ID, access to and uses of sensitive personal information would inevitably expand. Law enforcement, tax collectors, and other government agencies would want use of the data. Employers, landlords, insurers, credit agencies, mortgage brokers, direct mailers, private investigators, civil litigants, and a long list of other private parties would also begin using the ID and even the database, further eroding the privacy that Americans rightly expect in their personal lives. It would take us even further toward a surveillance society that would significantly diminish the freedom and privacy of law-abiding people in the United States. A national ID would foster new forms of discrimination and harassment. The ID could be used to stop, question, or challenge anyone perceived as looking or sounding "foreign" or individuals of a certain religious affiliation.

The Fiscal Year 2002 House Transportation Appropriations' report encourages the Department to study and define "the types of encoded data that should be placed on drivers' licenses for security purposes, and to work in concert with the states toward early implementation of such measures." These guidelines could be the first step toward federal involvement in the standardization of state drivers' licenses and the implementation of a national ID. We urge you to make recommendations that would provide the states with a series of security options rather than one uniform standard that could lead to a national ID.

In addition to our concerns raised in that coalition letter, the Free Congress Foundation would like to stress that a proposal to standardize procedures is not a substitute for increasing standards. Richard Clarke, whom President Bush appointed last October as the chairman of the new Critical Infrastructure Protection Board, has been openly dismissive of the alleged benefits of a National ID proposal and commented last year that he could not name one Bush official who supported the idea proposed by Oracle Chairman and CEO Larry Ellison[5]. Mr. Clarke has also been clear that more laws for improved computer security standards are unnecessary, "On the government systems side, we already have a lot of authority to issue standards and enforce them—we've never done that."[6]

The effect of standardizing procedures at a time of great technological change risks truncating the discovery process. The debate over biometric identifiers and

[5] Mills Abreau, Elinor, "Cyber-security czar snubs id plan, defends Govnet," Reuters, November 8, 2001.
[6] McCullagh, Declan, "The Sentinel," Wired magazine, p. 110, March 2002.

the networking of databases only highlights that new capabilities from technological and other developments are constantly appearing. Adopting a single standard not only locks us in to a system that might or might not be the best system we could adopt now but it also locks us out of learning what applications of what new developments are best and should be more widely adopted.[7] Allowing the states to act as laboratories of democracy better assures us of the benefits of discovering the best applications of new technologies.

Networking the state driver's license databases could create more problems than it would solve. Reconciling different databases such as with Social Security Numbers could be expected to generate errors in approximately 20% of the cases because of the use of nicknames . . . unmarried names, data entry errors, etc. on the social security record."[8] The more databases are networked the greater the risk that our information integrity standards would race to the bottom. The burden required to change data formats to achieve uniformity would be untenable.

The more databases are networked the greater the potential problem of misuse or other abuse of the sensitive data. A prominent group of conservative organizations came together and worked on this and related questions over a period of months as a Task Force on Information Exchange and Financial Privacy which just came out with its Report on Financial Privacy, Law Enforcement and Terrorism.[9] These are complicated questions that require that we should proceed slowly.

There is a role that the federal government needs to play in this debate. The most important role for Congress now is to actively pursue its oversight responsibilities. A great deal has been made of the fact that some of the highjack suspects of the planes on September 11th last year had U.S. driver's licenses. However, it was also reported that up to five of the men used stolen passports and that the U.S. State Department does not keep a list of passports that are reported stolen.[10]

---

[7] Stanley, Jay and Barry Steinhardt, "Drawing a Blank: The failure of facial recognition technology in Tampa, Florida," An ACLU Special Report, January 3, 2002. http://www.aclu.org/issues/privacy/drawing_blank.pdf

[8] Serian, Betty, Deputy Secretary of the Pennsylvania Department of Transportation, later Chair of the AAMVA Task Force on Identification Security, in a letter to the National Highway Traffic Safety Administration, Department of Transportation, July 31, 1998. http://www.epic.org/privacy/id_cards/penndot_letter_to_dot_ref.html.

[9] For the full report please see: http://www.prosperity-institute.org/projects/PI-TF-Report.pdf.

[10] "Use of stolen passport by highjackers: problems with Dept of State not keeping track," CNN.com, November 23, 2001. http://www.cnn.com/2001/US/11/23/inv.attacks.visas/index.html. See also Schemo, Diana Jean and Robert Pear, "Loopholes in Immigration Policy Worked in Hijack Suspects' Favor," September 27, 2001. http://college4.nytimes.com/guests/articles/2001/09/27/870395.xml

In addition, the Immigration and Naturalization Service needs to do a better job screening applicants.[11] Standardizing state driver's licenses and networking them with federal databases of false information only magnifies the problems. The networking of the current state of affairs with I.N.S. data integrity would only exacerbate errors. The letters sent recently notifying Mohamed Atta and Marwan Al-Shehhi (two men who flew planes into the World Trade Center) by the I.N.S. illustrates this point.[12] We are also concerned that calls for a national ID for foreigners would not only divert attention from the need to increase standards there but could foreshadow calls for a national ID for citizens as well.

In conclusion, I applaud the subcommittee for taking an active role in such an important question. The development of new technologies, including biometrics, might be able to improve the quality of our identification systems but their capabilities should not be exaggerated.[13] The focus of the federal government at this point should be to address the inadequacies of their own systems. Thank you again for this opportunity.

[11] Phyllis Schafly, Eagle Forum letter to Representative Horn, November 15, 2001.
[12] Potter, Mark and Rich Phillips, CNN, "INS issuance of flight school visas to two terrorists recently: Six months after Sept. 11, hijackers' visa approval letters received," March 13, 2002. http://www.cnn.com/2002/US/03/12/inv.flight.school.visas/index.html.
[13] Cole, Simon, "The Myth of Fingerprints," The New York Times, May 13, 2001. http://www.truthinjustice.org/fingerprint-myth.htm.

Forged Documents (Identity Cards, Record Books, Passports)*

The following security precautions should be taken:

* * * * *

2. All documents of the undercover brother, such as identity cards and passport, should be falsified.

3. When the undercover brother is traveling with a certain identity card or passport, he should know all pertinent [information] such as the name, profession, and place of residence.

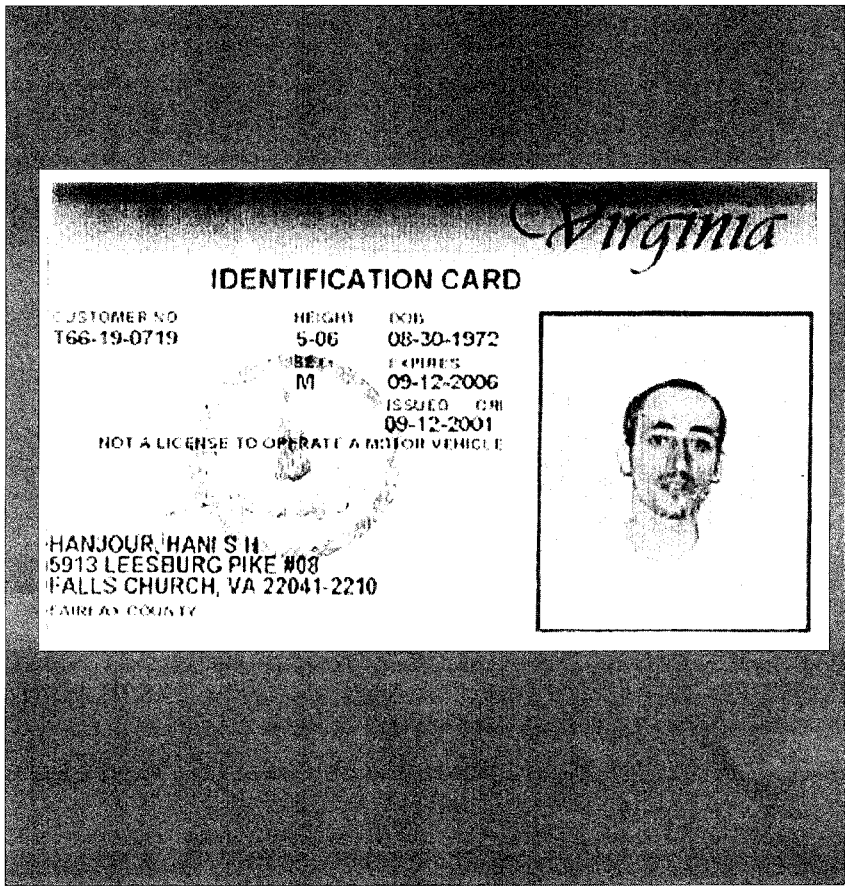
* * * * *

5. The photograph of the brother in these documents should be without a beard. It is preferable that the brother's public photograph [on these documents] be also without a beard. If he already has one [document] showing a photograph with a beard, he should replace it.

6. When using an identity document in different names, no more than one such document should be carried at one time.

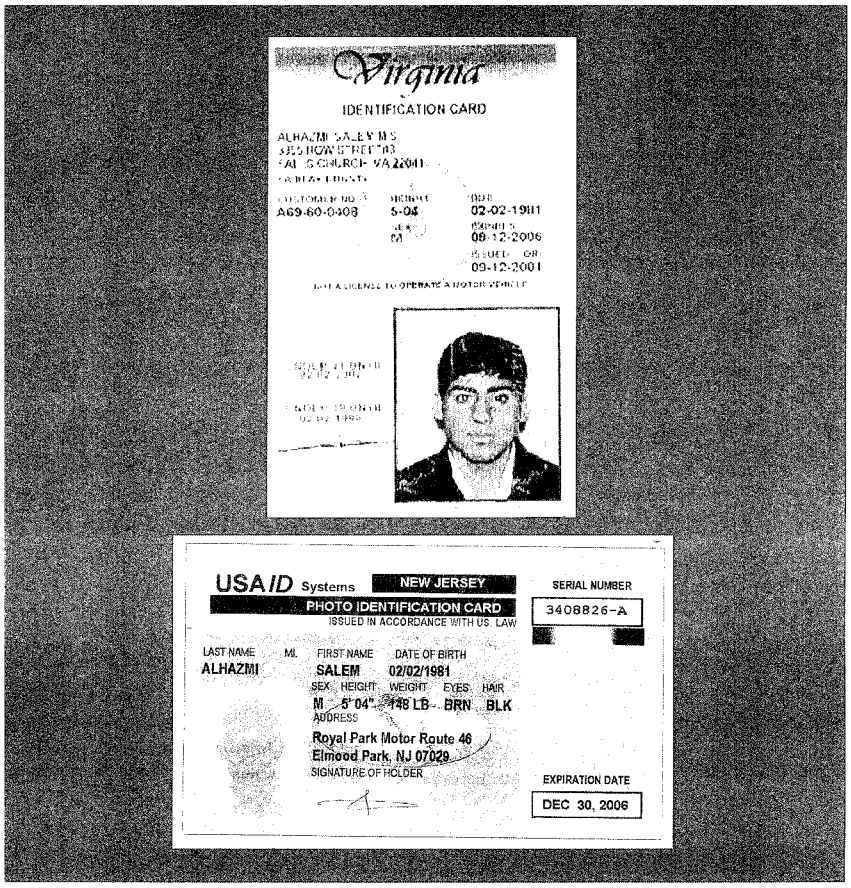
* * * * *

* The *Al Qaeda* Manual was located by the Manchester (England) Metropolitan Police during a search of an *al Qaeda* member's home. The manual was found in a computer file described as "the military series" related to the "Declaration of Jihad." The manual was translated into English and was introduced earlier this year at the embassy bombing trial in New York.

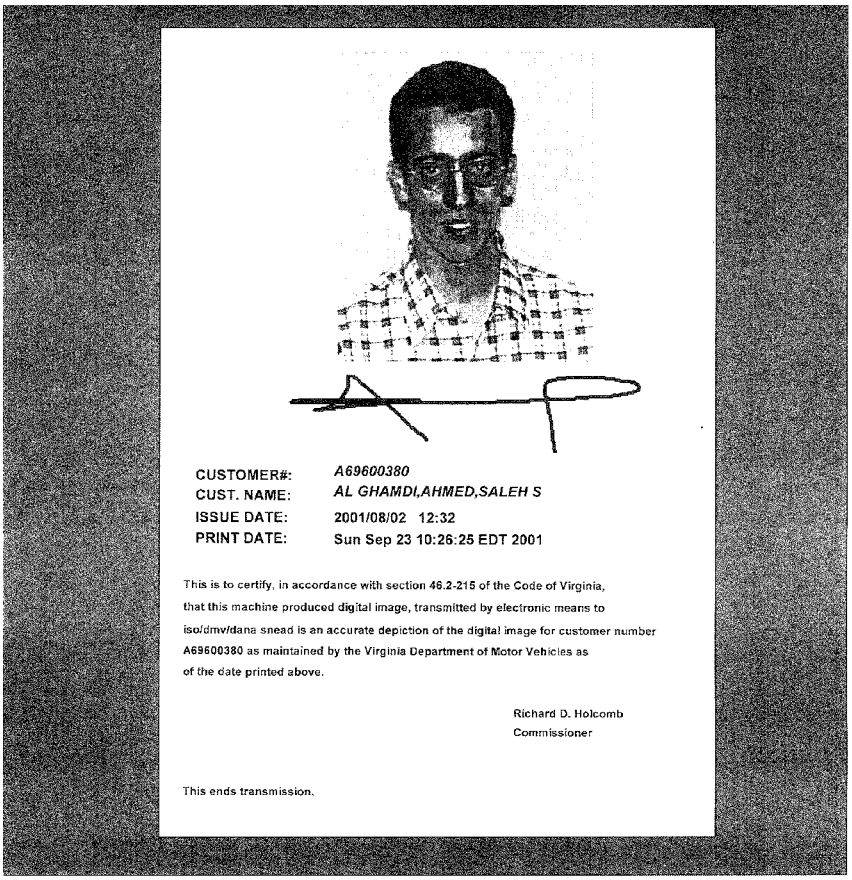


Hani Hanjour

Khalid Al-Midhar



Salem Alhazmi



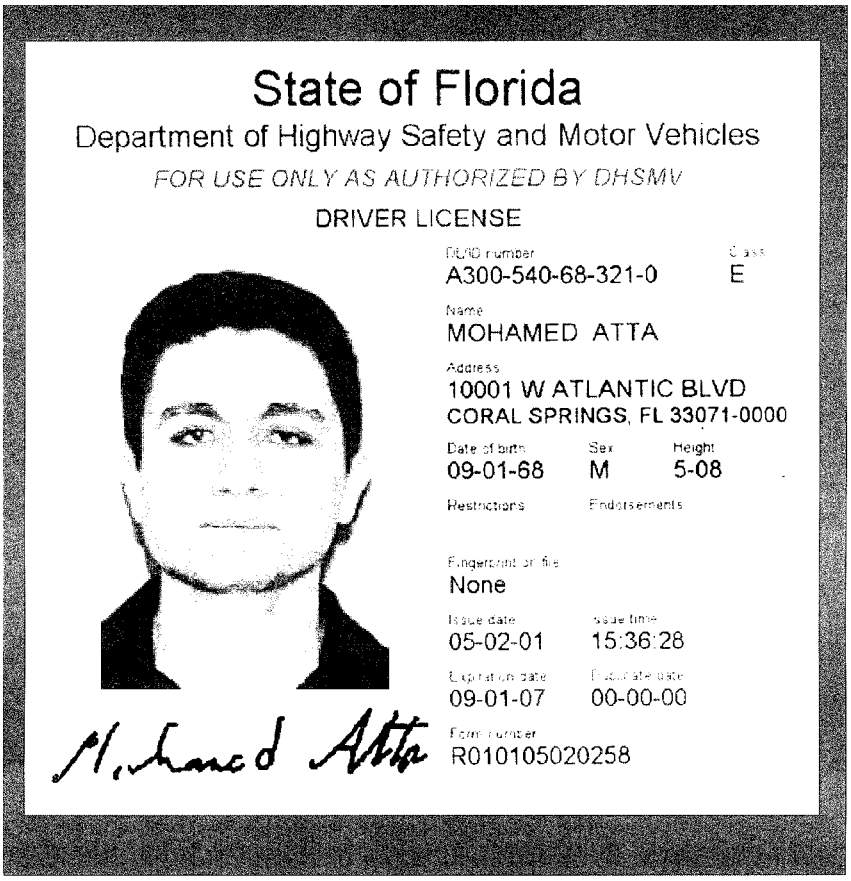
CUSTOMER#: *A69600380*
CUST. NAME: *AL GHAMDI,AHMED,SALEH S*
ISSUE DATE: 2001/08/02 12:32
PRINT DATE: Sun Sep 23 10:26:25 EDT 2001

This is to certify, in accordance with section 46.2-215 of the Code of Virginia, that this machine produced digital image, transmitted by electronic means to iso/dmv/dana snead is an accurate depiction of the digital image for customer number A69600380 as maintained by the Virginia Department of Motor Vehicles as of the date printed above.

Richard D. Holcomb
Commissioner

This ends transmission.

Ahmed Alghamdi



State of Florida

Department of Highway Safety and Motor Vehicles

FOR USE ONLY AS AUTHORIZED BY DHSMV

DRIVER LICENSE

DL/ID number
A300-540-68-321-0

Class
E

Name
MOHAMED ATTA

Address
10001 W ATLANTIC BLVD
CORAL SPRINGS, FL 33071-0000

Date of birth
09-01-68

Sex
M

Height
5-08

Restrictions

Endorsements

Fingerprint on file
None

Issue date
05-02-01

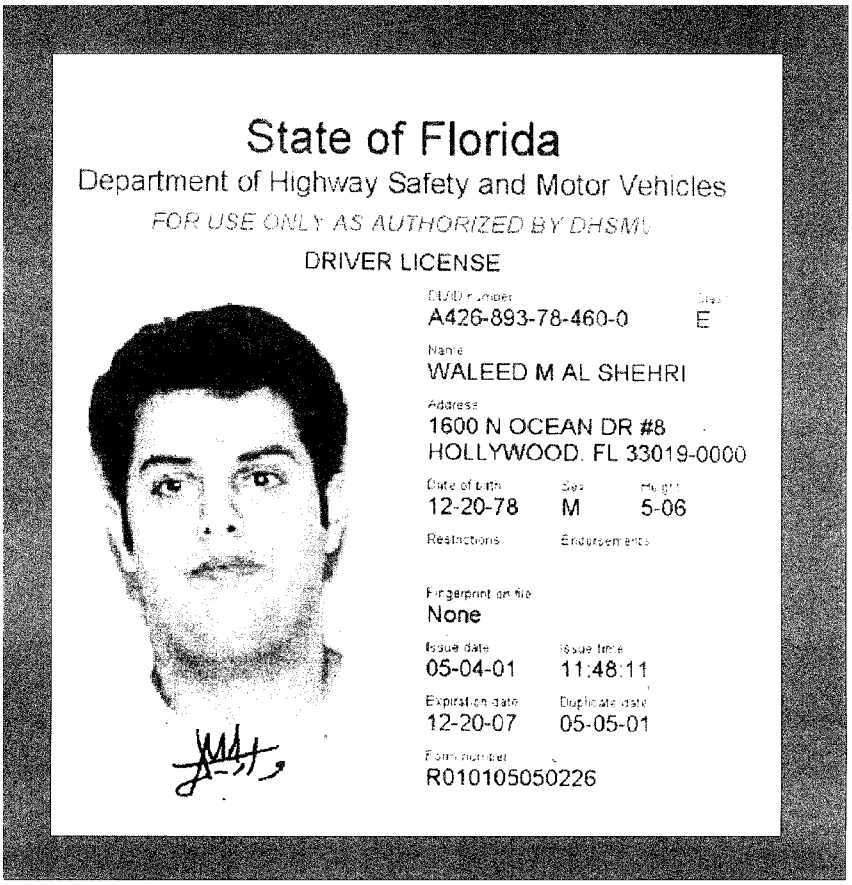
Issue time
15:36:28

Expiration date
09-01-07

Duplicate date
00-00-00

Form number
R010105020258

Mohamed Atta



State of Florida

Department of Highway Safety and Motor Vehicles

FOR USE ONLY AS AUTHORIZED BY DHSMV

DRIVER LICENSE

DLN/Number
A426-893-78-460-0

Class
E

Name
WALEED M AL SHEHRI

Address
1600 N OCEAN DR #8
HOLLYWOOD, FL 33019-0000

Date of birth
12-20-78

Sex
M

Height
5-06

Restrictions

Endorsements

Fingerprint on file
None

Issue date
05-04-01

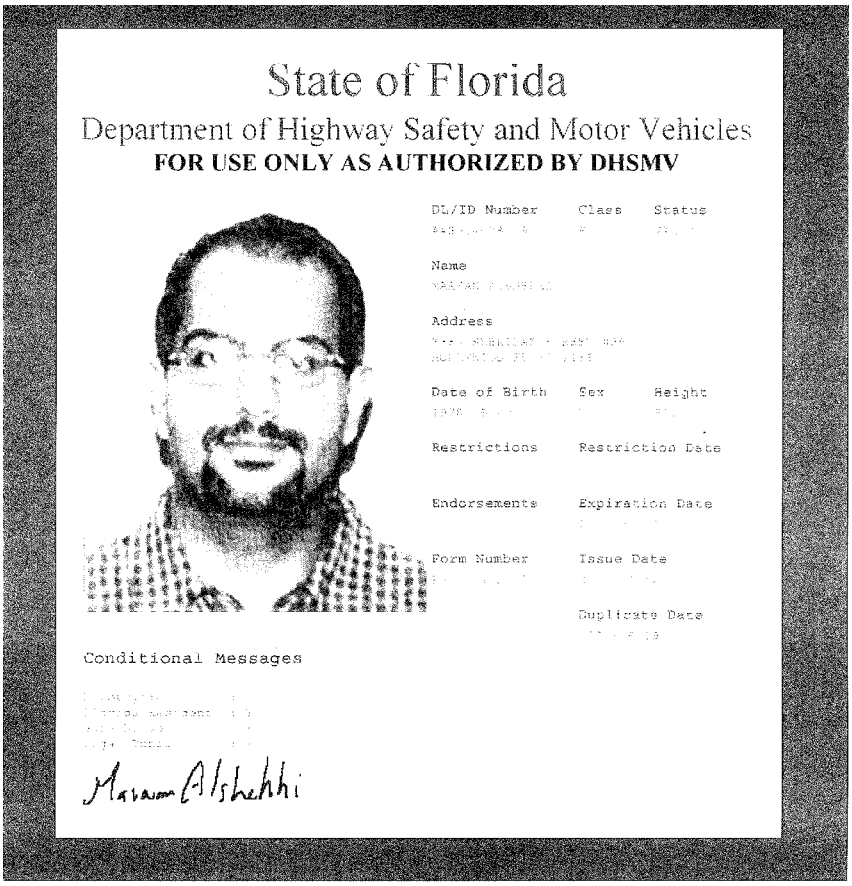
Issue time
11:48:11

Expiration date
12-20-07

Duplicate date
05-05-01

Form number
R010105050226

Waleed M. Alshehri



State of Florida

Department of Highway Safety and Motor Vehicles

FOR USE ONLY AS AUTHORIZED BY DHSMV

DL/ID Number Class Status

Name

Address

Date of Birth Sex Height

Restrictions Restriction Date

Endorsements Expiration Date

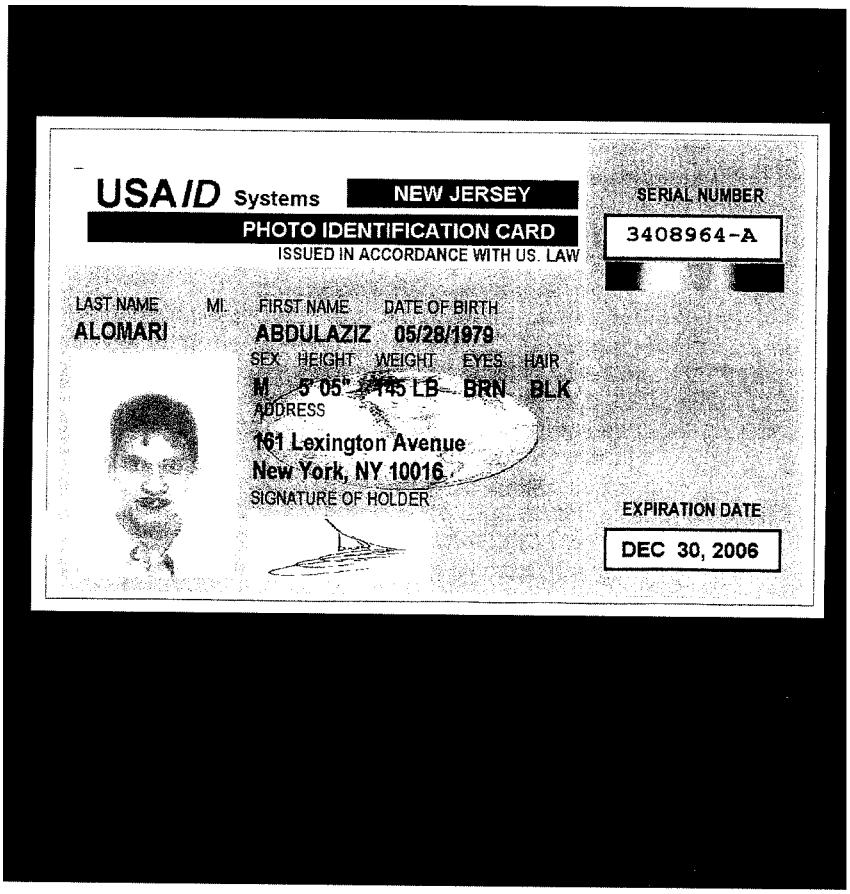
Form Number Issue Date

Duplicate Date

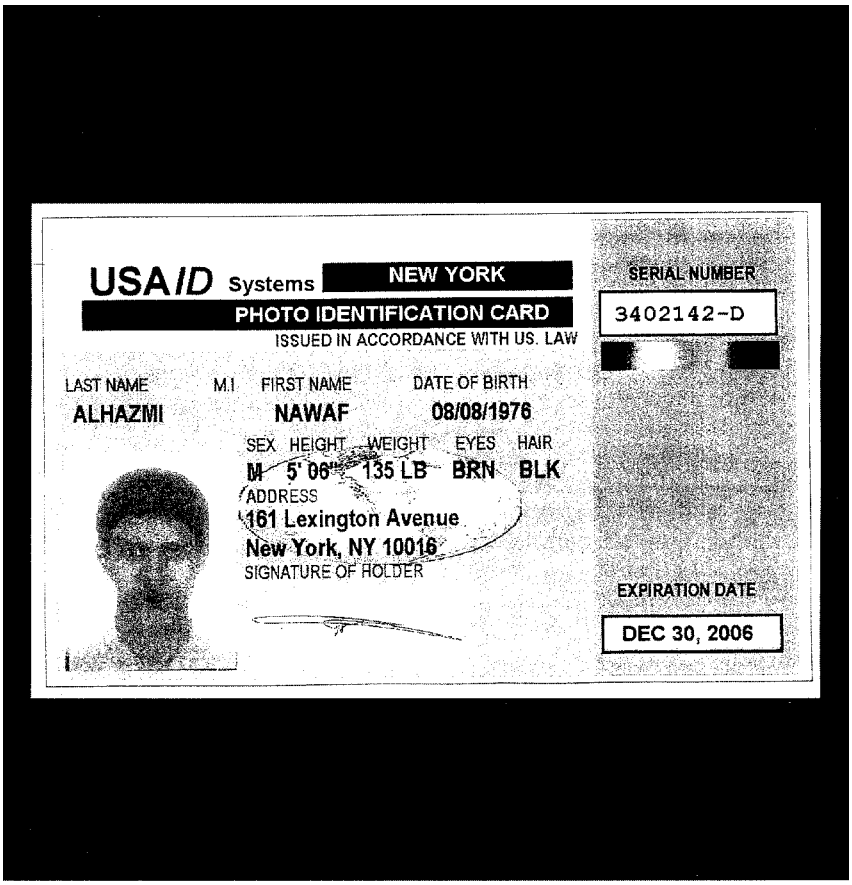
Conditional Messages

Marwan Al-Shehhi

Marwan Al-Shehhi



Abdulaziz Alomari

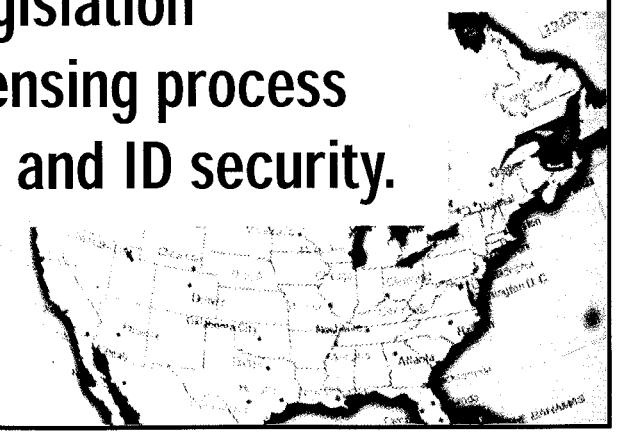


Nawaf Alhazmi

AAMVA
HELPING SECURE A SAFER AMERICA

77% of Americans FAVOR

Congressional legislation to modify the licensing process and ID security.



SOURCE: April 2002 Public Opinion Poll conducted by Public Opinion Strategies

AAMVA
American Association of Motor Vehicle Administrators

Testimony of the
Food Marketing Institute

"A License to Break the Law?"

Protecting the Integrity of the Driver's License

United States Senate Committee on Governmental Affairs
Oversight of Government Management, Restructuring and the District of Columbia Subcommittee

April 16, 2002

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to submit testimony on behalf of the 2,300 member companies and the 26,000 retail food stores represented by the Food Marketing Institute (FMI). Neighborhood grocery stores are very interested in the integrity of driver's licenses and applaud the efforts of this Subcommittee in looking at this important issue.

The driver's license has become a de facto identification card for a host of purposes at the supermarket. Some of these functions are required by government regulations, like age verification for purchasers of alcohol or tobacco products or verification of identification for our industry's 3.5 million employees. Other uses of the driver's license include being an important tool for business decisions, like deciding to cash or accept a customer's check. New regulations by the U.S. Treasury Department may impose additional identification verification requirements for certain types of financial transactions.

While strongly supporting the effort to improve the integrity of the driver's license, the food retail industry asks that the following considerations be made to allow for immediate utilization of the existing infrastructure to improve the integrity of the identification process:

1) Retailers should not be prohibited from verifying and recording necessary information from the driver's license for identity or age verification purposes.
2) The standardization of all state driver's licenses should include a magnetic stripe in addition to any other emerging technologies that may be added. Magnetic stripe technology is available in most stores immediately. It will likely take years to achieve mass adoption of any emerging technology such as smart card or biometric identification in supermarket check out lanes.
3) No proprietary hardware or data standards should be approved as the only entity or process to facilitate standardization.

4) Date of birth information should be contained on track 2 of the magnetic stripe where it can be read by retail establishments today. All stores with magnetic stripe readers can read data on track 2. Only a limited number of stores are also capable of reading track 3 with current equipment.

These four considerations will allow for immediate utilization of the existing magnetic stripe infrastructure found in retail establishments to improve the integrity of the identification process.

Should a magnetic stripe not be available on the driver's license card, or should the information be contained on track 3 instead of track 2, a full scale equipment upgrade would be necessary for supermarkets to read the information, which would come at a cost of $175 million dollars for just the supermarket segment of the retail industry.

We would be pleased to discuss these issues with you or your staff in more depth.

A License to Break the Law?
Protecting the Integrity of Driver's Licenses

Testimony submitted to:

Governmental Affairs Committee
Subcommittee on Oversight of Government Management,
Restructuring and the District of Columbia
U.S. Senate

Presented by

Raul Yzaguirre
President and CEO

National Council of La Raza
1111 19th St., NW, Suite 1000
Washington, DC 20036
(202) 785-1670

April 16, 2002

I. Introduction

The National Council of La Raza (NCLR) is the largest constituency-based national Hispanic civil rights organization in the United States. NCLR is an "umbrella organization" for more than 270 local affiliated community-based organizations (CBOs) and has a broader network of 30,000 groups and individuals nationwide. In addition to providing capacity-building assistance to our affiliates and essential information to our individual associates, NCLR serves as a voice for all Hispanic subgroups in all regions of the country. Over the past several months, we have received many calls regarding restrictive driver's license proposals in the states; communities are very concerned and have mobilized in states as diverse as Florida, Tennessee, California, and Washington to defeat potentially harmful legislation. This issue is fundamentally important to our community and affects individuals and families on a daily basis. For that reason, NCLR is grateful for this opportunity to submit testimony with respect to proposals to standardize driver's licenses across the country.

In the post-September 11 environment, the debate over driver's licenses has been linked to issues of national security. NCLR firmly believes that national security is of the utmost importance. Furthermore, NCLR agrees that driver's licenses must be valid and reliable documents that accurately prove one's identity, and supports measures to increase the integrity of driver's licenses and state-issued identification documents. However, we fear that restrictions on immigrants' access to driver's licenses may become part of this debate at the national level. Already we have seen a plethora of legislation, executive orders, and regulatory changes in the states which impose harsh restrictions specifically on immigrants' access to state-issued driver's licenses and identification documents. The impact on the Latino population is potentially enormous. These proposals go well beyond denying undocumented immigrants access to driver's licenses and have the potential to exclude legal immigrants and even U.S. citizens from state-issued identification documents. Moreover, these proposals are of great concern because they prohibit drivers from being properly licensed and insured, discriminate against immigrants and other groups, and make entire communities less safe.

NCLR believes that a state-issued driver's license should be reliable proof of an individual's identity and proof of authorization to drive a motor vehicle; it should not be tied to an individual's immigration status. There are legitimate and sound avenues for individuals to prove identity which would allow state Departments of Motor Vehicles to fulfill their mission of ensuring safe roads without creating new licensing requirements that would make the driver's license a *de facto* proof of legal residency in the United States.

We urge Congress not to enact legislation that would require state driver's licensing agencies to check and verify the immigration status of individuals applying for driver's licenses.

II. An Overview of Federal and State Driver's License Requirements

State driver's license agencies have a twofold task: licensing qualified motorists and ensuring the validity of driver's licenses. Each individual state licensing agency has distinct policies and procedures to which applicants must adhere before a license will be issued.

Current federal law does not require states to deny driver's licenses to undocumented immigrants, and very few state statutes contain language explicitly denying driver's licenses to undocumented immigrants or requiring lawful presence in the U.S. However, some state driver's license requirements, such as the requirement to provide Social Security Numbers (SSNs), have resulted in the inability of undocumented immigrants in some states to receive driver's licenses, rendering them unable to participate in proper driver education courses, to obtain insurance, and to perform daily activities. In some cases, legal immigrants have also been unable to provide the necessary documentation to obtain a driver's license.

Social Security Number Requirements

Many states require driver's license applicants to provide an SSN, and many states believe that they must require SSNs in order to be in full compliance with federal law. However, the federal SSN requirements are frequently misunderstood. Briefly, the Personal Responsibility and Work Opportunity Reconciliation Act (PRWORA) of 1996 contained a provision requesting that state driver's license agencies record the SSN of applicants for driver's licenses for the purpose of child support enforcement. Specifically, Section 466(a)(13)(A) directed that SSNs be recorded on applications for professional licenses, commercial driver's licenses, occupational licenses, and marriage licenses (and was later amended to include all licenses). The Department of Health and Human Services interpreted this provision to mean that states must have procedures to obtain the SSNs of any individuals who have SSNs, but not that an SSN be a requirement for driver's licenses. However, many states' statutes now contain language requiring that driver's license applicants provide SSNs. Because of the SSN requirements, many immigrants are unable to obtain driver's licenses.

Effective March 1, 2002, the Social Security Administration will no longer assign SSNs when the sole reason for needing an SSN is to obtain a driver's license. Prior to March 1, the SSA would assign SSNs to lawful residents who did not have work authorization but needed a valid SSN for non-work-related reasons, such as acquiring a driver's license. This new policy means that people who are lawfully present in the U.S. but are not authorized to work will no longer be able to obtain an SSN and will therefore be unable to obtain a driver's license in many states.[1]

Proof of Identity and Residency Requirements

Besides providing an SSN, applicants for a state-issued driver's license must also provide proof of age and identity and, in some instances, proof of state and legal residency. Often, these are intertwined, and many states' proof of identity requirements serve as a *de facto* means of probing into a noncitizen's immigration status by limiting the types of Immigration and Naturalization Service (INS) documents accepted as proof of identity.

[1] See "Frequently-Asked Questions about SSNs for Driver's Licenses," http://www.SSA.gov

Proof of Identity

Each state has its own list of acceptable documents for proving one's identity. Unfortunately, in many states, the list of documents accepted to verify identity is unnecessarily narrow and is an obstacle for many noncitizens who are at various stages of the immigration process and who do not have the accepted documentation. As a result, some immigrants remain unable to produce the required documentation to prove their identity and therefore are ineligible to receive a driver's license.

There are many documents that can be used as proof of identity, including driver's licenses issued by other states or countries, U.S. passports, U.S. original state birth certificates, state ID cards, student ID cards, original Social Security cards, U.S. military photo ID cards, Indian tribal photo ID cards, and some INS documents, such as a Certificate of Naturalization, an Arrival-Departure Record (I-94), an Alien Registration Receipt Card (I-551), a Letter of Authorization issued by the INS, a visa, or a valid Employment Authorization Card (I-688 A or B). In several states, Canadian driver's licenses, passports, and birth certificates can be presented as proof of identity in the same manner as another U.S. state's or territory's driver's license or birth certificate. A few states accept documents issued by Germany and France. However, these same documents from other countries may or may not be accepted, resulting in an inequity for noncitizens from most every country in the world.

Proof of State Residency

Some states explicitly require proof of residency in the state. These states require documentation to prove that the individual lives in the state, such as a utility bill, a bank statement, a rent receipt, an insurance policy statement, or a tax receipt. However, proving residency can be difficult for many individuals, particularly when more than one person lives in the same house or apartment and utility bills and rent receipts are often under only one occupant's name. Furthermore, many immigrants do not have bank accounts, insurance policies, or access to other acceptable documents. As a result, many immigrants are ineligible for driver's licenses because they cannot prove state residency.

Proof of Legal Immigration Status

In addition to state residency, a few states explicitly require proof of legal immigration status or proof of legal residency in the United States. Many more states are currently seeking to require legal immigration status. Currently, California explicitly requires proof of legal presence in the United States. Other states are less explicit. For example, in South Carolina the statute denies driver's licenses to anyone "who is not a resident of South Carolina, except for persons from other countries who are present in South Carolina on a student visa or on a work visa or the dependents of the student or worker who may be issued a license."[2] Following September 11, the South Carolina Department of Motor Vehicles (DMV) began to interpret this provision more narrowly and no longer grants driver's licenses to immigrants without green cards, valid student visas, or work visas, or to dependents of persons with the proper documentation. Although in

[2] South Carolina Code Ann. Section 56-1-40 (7).

most states legal immigration status is not explicitly required, undocumented immigrants are denied access to driver's licenses because they cannot meet the proof of SSN, proof of identity, or proof of state residency requirements.

In summary, because of documentation requirements, undocumented immigrants and other immigrants have been unable to obtain driver's licenses in many states. The implications are wide-ranging, and the impact is felt by individuals and entire communities. As a result of current law, many unlicensed drivers are currently driving on U.S. roads creating unsafe conditions for all Americans. Because the need to travel does not diminish if a driver's license has been denied, many individuals will continue to drive without driver's licenses and thus without proper driver's education and without insurance. Furthermore, unlicensed and uninsured drivers are more likely to flee the scene of an accident even if not at fault. And since driver's license databases are often used to enforce child support payment and criminal warrants, many remain immune from these law enforcement mechanisms. In many states, the driver's license agency issues not only driver's licenses but also official identification. Often, the requirements for a state ID are similar to those for a driver's license. Therefore, access to a driver's license is commensurate with access to a common proof of identity. Without state-issued identification documents it may be difficult to accomplish the tasks necessary for everyday life, such as opening a bank account and cashing a check.

III. Current Restrictive Proposals

Over the past several years, local police forces, Departments of Transportation, insurance companies, employers, community advocates, and others have launched campaigns to make driver's licenses more accessible to all people and thus improve public safety. Successful campaigns in Utah and Tennessee, and an ongoing campaign in California, have sparked campaigns in other states.

After the tragic events of September 11, 2001 and revelations that several of the terrorists had obtained state-issued driver's licenses, there has been renewed debate over immigrants' access to driver's licenses and state identity documents. Over the past several months, the list of states with restrictive proposals grew daily, and the types of immigrant restrictions proposed increase as well. Most alarmingly, these new proposals go well beyond requiring legal immigration status and create situations in which noncitizens are treated distinctly from citizens, resulting in discrimination and civil rights violations. The following outlines the major categories of immigrant restrictions that have been proposed in recent months:

- **Lawful presence requirements.** Several states have introduced legislation that explicitly requires driver's license applicants to prove that they are lawfully present in the U.S., thereby excluding undocumented immigrants from receiving driver's licenses. These proposals often contain narrow lists of acceptable documents for proving lawful presence which also exclude many legal immigrants.

- **Distinct processes for noncitizen applicants**. Several states have proposed that all noncitizens, even long-time legal permanent residents, be required to go to particular DMV

offices in order to apply for a driver's license or state ID card. These proposals may contain provisions requiring specialized training for DMV staff in the noncitizen facilities.

- **Strict photograph requirements.** Several states propose to overturn laws allowing individuals to refuse photographs on religious or other grounds.

- **Document verification requirements.** Several states have introduced proposals requiring the DMV to verify noncitizens' documents with the Social Security Administration database and/or the INS database, neither of which are designed for this purpose and are fraught with inaccuracies that result in denial of eligible applicants.

- **Reporting requirements.** Several states have new proposals requiring and/or allowing DMVs to share information regarding "suspicious" applicants with the appropriate state and/or federal law enforcement agency.

- **Driver's license expiration date requirements.** Several states have proposals to require that driver's licenses expire the same day as an individual's visa.

- **Repeal of expansive legislation.** There have been efforts to repeal laws allowing Individual Taxpayer Identification Numbers (ITINs) to be used as a substitute for SSNs, thereby requiring individuals to have a valid SSN.

- **Revocation for misrepresentation of immigration status.** Several states have proposals that would require the DMV to revoke the driver's licenses of individuals who have misrepresented their immigration status.

- **Biometric data.** Several states have new proposals with provisions requiring biometric data, such as fingerprints, to be collected and used on driver's licenses.

- **Immigration status listed on driver's license.** Several states have proposed steps to indicate immigration status on the face of the driver's license or to create new driver's licenses that differentiate between undocumented immigrants, noncitizens, and citizens.

IV. NCLR Principles

Like all Americans, NCLR is concerned about national security and supports measures that increase the safety of the U.S. and protect Americans from future terrorist attacks. However, NCLR firmly believes that, before taking antiterrorist action, it is necessary to reflect on whether a proposed measure is truly an effective means to increase national security, as well as to address unintended negative effects of such proposals.

During these challenging times, many new proposals aimed at enhancing our national security and preventing future terrorist attacks have arisen. However, we must be cautious not to proceed quickly and recklessly. NCLR believes that each new state and federal legislative proposal and

executive action must receive thoughtful attention, broad discussion, and be judged by four principles. Specifically,

A. **Driver's license proposals must be effective.** Will the proposal achieve what it intends? Is it an effective means to achieve greater national security and public safety, or does it give us a false sense of security and simply make us feel better? Is the proposal cost-effective, or would we expend a great amount of resources on unproven or ineffective results?

B. **Driver's license proposals must not create negative unintended consequences.** What are the ultimate results of the proposal? Will the proposal deny driver's licenses to eligible individuals?

C. **Driver's license proposals must not single people out for abuse and discrimination.** Will the proposal create opportunities for abuse, or result in discrimination or civil rights violations? Are there ample protections contained in the proposal to protect individuals from abuse?

D. **Driver's license proposals must be based on accurate information.** Will the proposed changes ensure that the information contained on a driver's license or identity document is accurate? If the information is to be verified with databases, is the information contained in the database reliable and accurate? Is the identity document based on information from valid documents?

NCLR believes that these four principles should guide national and state debates on driver's license proposals and, indeed, any proposals aimed at enhancing safety and security. The vast majority of current driver's license proposals in the states fail to meet these standards.

V. Applying NCLR Principles to Current Proposals

While NCLR is deeply concerned with national security and public safety, it believes that current proposals to restrict state-issued driver's licenses and identification documents are not an effective means to combat terrorism. In fact, NCLR's position is that all communities' best interests are served by increased accessibility to identification documents. Furthermore, NCLR believes that driver's licenses should accurately and reliably identify individuals and should indicate an individual's authorization to operate a motor vehicle. However, driver's licenses should not be linked to an individual's immigration status. NCLR's analysis, as outlined below, suggests that current restrictive proposals could result in negative consequences and inaccurate information that would do little to enhance national security.

A. Driver's license restrictions are not effective.

- **Restricting driver's licenses is an inefficient and ineffective measure to prevent terrorism**. Sophisticated terrorists with substantial financial resources are likely to have the ability to obtain driver's licenses and other documents when they find them necessary.

Furthermore, press accounts since September 11 have called attention to the fact that the hijackers had obtained driver's licenses when, in fact, the terrorists did not need U.S.-issued driver's licenses to board planes on September 11; they had foreign passports that allowed them to board airplanes. Because of the large number of tourists and other visitors who travel in the U.S., foreign passports are likely to continue to be acceptable forms of identification to board airplanes. Finally, restricting driver's licenses to immigrants does nothing to address the issue of domestic terrorist threats.

The argument that identification cards can prevent terrorism is based on the premise that we can identify terrorists and separate the "good guys" from the "bad guys." However, it is first necessary for various federal agencies to gather intelligence and share information with each other in order to identify potential threats and stop them before they enter the U.S. Federal legislation has been proposed to increase intelligence-gathering and information-sharing at the federal level, and to revamp the visa issuance process. The nation's resources and energies are best spent gathering information and identifying potential terrorists rather than placing unnecessary driver's license restrictions on millions of American families.

- **Restricting driver's licenses interferes with other law enforcement mechanisms.** Law enforcement officials point out that the current child support enforcement and criminal warrant tracking functions of driver's licenses are less useful if large proportions of the population are excluded from the driver's license databases.

- **Restricting driver's licenses does not accomplish immigration policy goals such as reducing undocumented employment or improper use of public benefits.** A driver's license only proves identity and ensures that the license holder has shown a minimal level of competency to drive and understands U.S. traffic laws. Federal law requires all employees to complete an I-9 form, which requires both proof of identity and eligibility to work, so a driver's license alone is not enough. Furthermore, undocumented immigrants are ineligible for federal public benefits programs, and such programs require additional proof of eligibility, identity, and immigration status.

B. New driver's license restrictions have negative consequences for immigrants, citizens, and entire communities.

- **Driver's license restrictions result in the denial of licenses to legal immigrants.** Many of the current proposals would also effectively deny driver's licenses to many people who are authorized to live in the United States but who do not have the required documentation for a variety of reasons. For example, persons who have been given temporary protected status due to civil conflict or natural disaster in their countries, or abused women who are in the process of petitioning for legal residency under the provisions of the Violence Against Women Act, or individuals whose visas have been approved but not processed would be denied driver's licenses even though they are lawfully present. Furthermore, refugees, asylees, and others who fled persecution without proper identification documents from their countries of birth would be denied driver's licenses. In some states, new proposals mean that naturalized citizens would be treated differently than native-born citizens and would be subject to onerous requirements, which is unfair and potentially unconstitutional.

- **Restricting driver's licenses results in unsafe roads, high insurance rates, and overwhelmed court systems.** Current proposals would result in more unlicensed drivers operating vehicles on U.S. roads. Currently, there are an estimated eight million undocumented immigrants in the United States, many of whom have to drive on U.S. roads in order to work, whether or not they have a driver's license. As a result of immigrant restrictions these drivers will not take driving classes or pass driving tests, will not be able to get insurance, and may be more likely to flee the scene of an accident for fear of immigration consequences unrelated to the accident. Nationally, chances are approximately 14 in 100 that if an insured car occupant is injured in an accident, an uninsured motorist caused the accident.[3] These proposed measures are likely to increase those numbers. In addition, immigrant license restrictions result in numerous arrests for minor traffic violations, clogging the public courts and diverting the time of law enforcement officers who would be better used protecting public safety.

- **Driver's license restrictions negatively affect American families.** According to the Urban Institute, one in ten children in the U.S. lives in a "mixed-status family," in which at least one parent is a noncitizen and one child is a citizen. Four out of five children of immigrants were born in the U.S., and two out of three children in families with one or more undocumented parents are citizens.[4] The impact of denying driver's licenses to immigrants reaches far beyond the undocumented community and even the immigrant community. Denying driver's licenses to immigrants negatively affects U.S. citizens and American families.

- **Restricting driver's licenses erodes community trust.** Rather than increasing security, driver's license restrictions result in a situation in which immigrants fear discrimination and being reported to the INS and therefore avoid contact with law enforcement; immigrants are unwilling to report crimes and assist local law enforcement in fighting criminal and terrorist activity. This decreases community trust and infringes upon efforts to fight crime and save lives. In most states, law enforcement officials are opposed to restrictions on driver's licenses, citing public safety, fraud prevention, battling corruption, and crime prevention.

- **Restricting driver's licenses results in the proliferation of false documents.** The production and sale of falsified documents are likely to increase if large numbers of immigrants are denied driver's licenses. Excluding individuals from legal driver's licenses creates conditions in which false documents and false identities will proliferate, meaning that we will have less accurate information about who is currently in the country.

C. Driver's license restrictions result in abuse and discrimination.

- **Driver's license restrictions result in discrimination and racial profiling.** Increased restrictions on immigrant driver's licenses are likely to result in racial profiling, vigilantism, and other forms of discrimination. When documents such as driver's licenses are believed to

[3] Insurance Research Council, *Uninsured Motorists 2000 Edition*, Malvern, PA: Insurance Research Council, 2001.
[4] Children of Immigrants Fact Sheet, The Urban Institute, December 2001.

be linked to immigration status, history has shown that Latinos and other ethnic minorities, as well as all people who look or sound "foreign," are the primary targets of document verification. For example, people believed to be "foreign" or who look like they might be "undocumented" because they fit a certain profile may be stopped solely to provide documents, an enforcement activity that clearly leads to racial profiling. And if new laws require DMVs to report "suspicious" individuals to the INS, the probability of abuse and discrimination will increase dramatically.

- **Driver's license restrictions result in civil rights violations.** Often, individuals who are asked to show documentation are U.S. citizens, and those suspected of being "undocumented" are legal immigrants, resulting in civil rights violations. Reports of discrimination and racial profiling have already been documented. Puerto Ricans, who are U.S. citizens, have been the targets of such discrimination and have been asked to show proof of citizenship, or even worse, their green cards. Naturalized citizens have also been asked to produce additional documentation. In several cases, the driver's licenses of naturalized citizens, U.S. citizens, refugees, and others have been confiscated when the individuals failed to present green cards or other proof of legal immigration status.

- **Driver's license restrictions result in vigilantism.** Another potential effect of the increasing anti-immigrant sentiment in the nation is vigilantism; that is, undue, and often illegal, enforcement of existing laws by ordinary citizens. In the aftermath of the terrorist attacks of September 11, incidents targeting persons perceived to be immigrants have become all too common. Airlines and others have reportedly participated in racial profiling by asking members of particular ethnic and racial groups to provide documentation. If driver's licenses or other documents are linked (or perceived to be linked) to immigration status, it is likely that even more merchants, restaurant owners, and others will request documentation before services will be provided.

- **Discrimination and racial profiling make the country less safe.** Racial profiling undermines the ability of law enforcement to enforce the law effectively. When an innocent individual's ethnicity is used to establish a cause for suspicion of a crime, then that individual – along with family members, friends, and neighbors – may lose trust in the integrity of law enforcement. As a result, the public safety may be placed in jeopardy because members of these communities are likely to fear harassment and abuse by the police and are thus less likely to seek police help when they legitimately need it: to report a crime or suspicious behavior, serve as a witness, or otherwise cooperate with law enforcement. Racial profiling not only violates civil rights, it also diverts essential resources, undermines the ability of law enforcement to enforce the law effectively, and makes everyone less safe.

D. New driver's license proposals do not guarantee accurate and reliable information.

- **Immigrant restrictions to driver's licenses do not address the issue of false breeder documents.** The information on a driver's license is only as good as the information provided by the applicant. If individuals use false documents to obtain valid state-issued

driver's licenses or ID cards, these proposals simply result in a false sense of security without addressing the real issue of identity fraud and theft.

- **Blanket information-sharing with the INS and SSA does not increase public safety.** Linking driver's license databases to the INS or the Social Security Administration to verify documents is likely to have harmful consequences. First, the accuracy and reliability of the databases are problematic. INS and SSA databases have been shown to have error rates approaching 20%.[5] The INS database is not updated quickly enough to contain current immigration status for all persons. For example, according to the INS, no U.S. citizens naturalized prior to 1972 appear in INS databases at all. Such individuals would be routinely denied driver's licenses under these procedures. Finally, innocent mistakes, such as the misspelling of "unusual" names, transposing given names and surnames, and inconsistent entry of multiple surnames, disproportionately occur with ethnic minorities. If verification against INS data is used by driver's license agencies, it is inevitable that eligible persons will be denied driver's licenses because of inaccuracies in the databases. Sharing information with the INS and SSA does not lead to increased public safety. If immigrants do not apply for driver's licenses because they fear discrimination or that they will be reported to the INS or other law enforcement agencies, this results in greater numbers of unlicensed and uninsured drivers and less contact between the community and the authorities. Consequently, the entire community is less safe.

VI. NCLR's Proposed Approach

Certainly, maintaining the authenticity and reliability of driver's licenses is critical, as is ensuring that unauthorized drivers do not endanger the safety of all people. Taking steps to increase national security is also important. NCLR believes that these goals can be accomplished without denying immigrants access to driver's licenses. The next sections review practical steps that can and should be taken to ensure maximum access to driver's licenses without endangering national security or public safety.

Alternatives to Documentation Requirements

One way to ensure driver's license accessibility to immigrants is to offer alternatives to documentation requirements. The following sections outline possible alternatives to SSN, proof of identity, and proof of legal residency requirements.

Alternatives to the SSN

There are ways that states can allow those individuals to qualify for driver's licenses without SSNs. Some states have provided alternatives to the SSN requirement, clearly demonstrating that they have chosen public safety as a principal guideline for inclusive driver's license policies.

---

[5] See *Racing Toward "Big Brother": Computer Verification, National ID Cards, and Immigration Control*, Washington, D.C.: National Council of La Raza, 1995.

Some states allow individuals who do not have SSNs to present a sworn affidavit stating that they do not have an SSN and are not eligible for one. Besides the sworn affidavit, additional options are currently being utilized in various states. For example, Texas currently accepts an L-676 letter in place of an SSN. An L-676 letter can be obtained through the SSA and states that an individual does not qualify for an SSN. Issued by local SSA offices, an L-676 letter can be obtained by persons who can prove their age, identity, and ineligibility to obtain an SSN.[6]

Other states have additional alternatives. In Utah, for example, driver's license applicants can submit an L-676 letter or an Individual Taxpayer Identification Number (ITIN) issued by the Internal Revenue Service (IRS) for federal tax collection purposes. The ITIN is a tax processing number that became available on July 1, 1996 for certain nonresident and resident aliens, their spouses, and dependents. Like the SSN, it is a nine-digit number and only individuals who are not eligible for an SSN can obtain an ITIN.[7]

Alternatives to proof of identity and proof of residency documents

As with the SSN, there are ways to increase immigrants' ability to produce necessary documentation. One solution is to broaden the list of acceptable identity documentation to include foreign documents.

Foreign-issued documents
As mentioned above, several states accept Canadian driver's licenses, passports, and birth certificates as proof of identity, and a few states accept documents from other countries. However, most often these same documents from other countries are not accepted. All states could accept legitimate foreign government-issued documents, thereby allowing more individuals to access driver's licenses.

In most countries, obtaining a passport or consular documents requires extensive documentation before issuance. For example, a Mexican consular document (*matricula*) requires (1) a certified copy of a Mexican birth certificate and (2) a picture ID. Both a foreign passport and consular document are easily recognizable and verifiable documents issued by an individual's country of origin. They provide both an identifiable photograph and the date of birth of an individual.

The acknowledged validity of the *matricula* has led some financial institutions and other entities to accept it as an alternative form to prove identity. In Orange Country, California, chiefs of police have adopted policies encouraging officers to accept the *matricula* as an alternative ID when stopping individuals for minor offenses. This measure is intended to diminish community reluctance to have contact with police or to report crimes.[8] Similarly, some banks allow customers to use it as one of two proof of identity documents to open bank accounts or effect transactions. Given that immigrants are vulnerable to robberies and predatory schemes because

[6] From Texas Register, September 22, 2000. Comments on rule changes to 37 Texas Administrative Code,
[7] *Understanding your IRS Individual Taxpayer Identification Number*, IRS Publication 1915, February 1999. http://www.irs.gov/ind_info/itin.html
[8] For example, see Teresa Puente, "Mexico ID like money in bank. Consul card a key to fiscal freedom," *Chicago Tribune*. March 18, 2002.

they do not have access to banking facilities, measures to facilitate their access to these services could also serve to reduce crime.

Likewise, original foreign birth certificates are carefully issued to individuals by national governments. Currently, several states accept foreign birth certificates as the only document required for identification purposes. Other acceptable foreign government-issued documents include a national military identification card, a voter registration card, driver's license, school records, or a variety of other documents.

State Departments of Motor Vehicles can work with foreign consulates to receive information and training regarding the documentation issued by any foreign country. Consulates can also provide helpful information regarding identifying false documents.

There are also alternative ways to prove state residency. For example, some community service organizations are willing to provide affidavits that can be notarized and used for proof of state residency. In addition, residents can request that newsletters or other pieces of mail be sent to them at their address to be used as proof of residency. Individuals and organizations need to check with their local driver's license agency to determine what types of proof of state residency are acceptable.

NCLR believes that state driver's license agencies should work to ensure that individuals who are driving on roads are licensed, insured, and knowledgeable of all rules, and should not act as INS agents by verifying immigration status. Given the identity and legal residence requirements, INS documentation and immigration law are extremely complex and subject to frequent changes. State driver's licensing agencies do not have the authority or the expertise to navigate through the variety of immigration documents and understand the nuances among different types of immigration status and stages of the process. These complexities have been brought to bear when agencies or legislators have adopted seemingly straightforward policies to prevent undocumented immigrants' access to driver's licenses, which have instead resulted in denying such documents to certain categories of legal immigrants.

VIII. Conclusion

Public safety and national security are of the utmost importance to all people of the United States, and measures to identify potential terrorists and prevent future terrorist attacks are a national priority. Safety and security goals are not mutually exclusive and can be accomplished through measures that carefully combine effectiveness, accuracy, explicit civil rights protections, and prevention of discriminatory effects. Steps must be taken to ensure that new policies are effective and truly make the country safer rather than simply make us feel better at the expense of innocent members of the population. Restricting immigrant access to driver's licenses is not an effective way to counter potential terrorists and actually makes the entire community less safe. Unfortunately, the Latino population is already all too familiar with discrimination, racial profiling, unsafe communities, and other negative effects of driver's license restrictions. NCLR seeks to make sure that these problems are not further exacerbated by legislation that would

require states to check and verify the immigration status of individuals applying for driver's licenses.

Allowing maximum access to state-issued ID cards and driver's licenses through legitimate means ensures that all drivers are properly trained, licensed, and insured. It provides all residents of the United States with documentation, increasing our knowledge of who is in the country at any given time and preventing large segments of the population from living clandestinely and avoiding contact with law enforcement and other government and private agencies.

State Departments of Motor Vehicles should not check the immigration status of driver's license applicants. The U.S. Constitution gives the federal government the sole authority to create and enforce immigration law; only the INS is responsible for issuing immigration documents and verifying the legal residency of persons residing in the United States. Furthermore, immigration law and immigration documents are incredibly complex and subject to frequent changes. State driver's licensing agencies do not have the expertise to navigate through the variety of immigration documents and verify an individual's immigration status. Doing so without expertise typically leads to discrimination against persons who are lawfully present in the U.S. The Department of Motor Vehicles' role should be to ensure that all individuals who drive on U.S. roads are properly licensed and insured, and not to act as INS agents verifying immigration status.

Ensuring immigrants access to driver's licenses ensures safer roads and safer communities.

Thank you again for this opportunity to present testimony.

www.lpa.org

April 16, 2002

Sen. Richard Durbin
Chairman, Subcommittee on Oversight of Government Management,
Restructuring, and the District of Columbia
601 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Durbin:

I am writing to request that the enclosed testimony of LPA be included as part of the hearing record for the Subcommittee's hearing today *Are You Really Who You Say You Are? Improving the Reliability of State-Issued Drivers' Licenses.*

As you may know, LPA is a public policy advocacy organization representing senior human resource executives of over 200 leading employers doing business in the United States. LPA provides in-depth information, analysis, and opinion regarding current situations and emerging trends in labor and employment policy among its member companies, policy makers, and the general public. Collectively, LPA members employ over 19 million people worldwide and over 12 percent of the U.S. private sector workforce. LPA member companies have revenue exceeding $4.3 trillion annually.

As is explained in more detail in our prepared testimony, the security challenges that LPA member companies are now facing are closely aligned with the security interests of the nation as a whole. We look forward to working with you as you and the other members of the Subcommittee address these important issues.

Please do not hesitate to contact me if LPA can be of assistance on these matters.

Sincerely yours,

Michael J. Eastman
Director, Government Relations

Enclosure

LPA, INC. 1015 FIFTEENTH STREET, NW SUITE 1200 WASHINGTON, DC 20005-2605
TEL 202.789.8670 FAX 202.789.0064 INFO@LPA.ORG

STATEMENT

OF

LPA

ARE YOU WHO YOU SAY YOU ARE? IMPROVING THE RELIABILITY OF STATE-ISSUED DRIVERS' LICENSES

BEFORE THE SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT, RESTRUCTURING, AND THE DISTRICT OF COLUMBIA

SENATE COMMITTEE ON GOVERNMENTAL AFFAIRS

WASHINGTON, DC

APRIL 16, 2002
(02-50)

1015 FIFTEENTH STREET | SUITE 1200
WASHINGTON DC 20005
202.789.8670 | FAX 202.789.0064 | WWW.LPA.ORG

Thank you for the opportunity to present the views of LPA regarding the deficiencies in the security of drivers' licenses and other forms of identification and the potential for bolstering the integrity of those systems.

As you may know, LPA is a public policy advocacy organization representing senior human resource executives of over 200 leading employers doing business in the United States. LPA provides in-depth information, analysis, and opinion regarding current situations and emerging trends in labor and employment policy among its member companies, policy makers, and the general public. Collectively, LPA members employ over 19 million people worldwide and over 12 percent of the U.S. private sector workforce. LPA member companies have revenue exceeding $4.3 trillion annually.

Since September 11, there is an increased emphasis on security issues in the workplace. This emphasis has resulted in a substantial number of initiatives at all levels of government intended to prevent a recurrence of similar incidents. Many of these initiatives have focused on identification documents because of the significant share of the September 11 terrorists who obtained fake or fraudulent drivers' licenses, visas, or Social Security cards.

Many of these new initiatives will have a significant impact on the efforts of American companies to address their own security needs, which are aligned with those of society as a whole. It is important that these governmental initiatives facilitate the establishment of human resource and data protection policies and procedures that address the pressing security needs facing America today in a workplace-friendly manner, while also protecting the privacy and confidentiality interests of employers and their employees.

Because of the profound implications for the American workplace, LPA has established a Workplace ID Advisory Board to provide expert advice on public policy proposals that will have an impact on corporate security and the protection of employees, employer facilities and informational infrastructures. The Board also examines security practices of American companies and is in the process of developing a protocol for corporate security policies that will provide guidance for companies in balancing their security needs with the privacy interests of their employees. This Board is composed of security, legal, human resource and technology experts to provide guidance to our organization in addressing the various proposals in play. This testimony reflects the views of those distinguished individuals.

LPA strongly supports efforts to improve the integrity of documents used for identification in the United States. Employers are already required by law to use various forms of identity documents to confirm whether individuals are eligible for employment. Existing procedures require employers to verify an individual's citizenship status or, if an alien, their visa status before employment commences. One of the most common documents used by employees to demonstrate their identities is the drivers' license. Yet, as reported by the General Accounting Office, in examining Immigration and Naturalization Service data for a 20 month period in the late 1990's, about 50,000 unauthorized aliens used about 78,000 fraudulent documents to obtain employment.[1] While most of these fraudulent documents were INS documents and Social Security cards, a sizable number were drivers' licenses.[2]

At the same time, employers are also facing increasing difficulties in proving the identity of their employees to customers and clients. As one LPA member recently reported, their salespeople visiting client companies are frequently prompted for photo identification. Typically these employees present a state-issued ID such as a drivers' license. However, increasingly clients are asking for a second photo ID, desiring more security than can be offered through existing drivers' licenses. This particular company is in the process of paying its employees expenses incurred in obtaining U.S. passports to ensure that they will be permitted access to client facilities.

Consequently, LPA applauds proposals, such as that of the American Association of Motor Vehicle Administrators (AAMVA), which takes several important first steps toward improving ID systems. LPA is particularly supportive of provisions to combat fraud, create unique individual identifiers, and link state databases with each other in a more efficient manner. We eagerly await the introduction of legislation in Congress to implement the AAMVA proposal and hope to work closely with Chairman Durbin and the other members of this Subcommittee to help shape such legislation to ensure that it accomplishes its laudable goals.

At the same time, while LPA is supportive of these steps, we must all recognize that domestic security cannot be ensured without more. Drivers' licenses and state-issued ID cards are a central component of identification and security systems in use in the United States today, but much more needs to be done to improve security. In particular, Congress should carefully consider the responsibilities that other institutions, such as private employers, bear in bolstering domestic security and should provide those institutions with appropriate tools so that they can effectively perform their responsibilities.

Corporate Security After September 11

As noted previously, because of the terrorist attacks of September 11, there is an increased emphasis on security issues in the workplace.

Chief among those concerns facing employers is how to provide a high level of assurance to employees, customers, clients, and the general public that they maintain safe and secure workplaces. The importance of this concern is underscored by a survey reported last month in the *Wall Street Journal*, in which corporate chief executives were asked to identify those areas that posed a much greater concern for them today than before September 11. Of those chief executives polled, 79 percent listed protection of employees as such a concern.[3]

One step that employers often use to bolster security is to verify the identity of employees, contractors, guests, and other individuals who access employer facilities. At the same time, employers often need to conduct background checks on employees, applicants, and others with access to the employer's premises. After September 11, employers are more routinely checking identity and implementing background checks, as is evidenced by reports that 51 percent of corporate chief executives report now conducting background checks on contract employees while 39 percent report now checking employee backgrounds more fully.[4]

Improving Integrity of IDs Critical to Security

Needless to say, verifying identity of those with access to employer facilities is now more important than ever to employers. Yet, those documents that individuals most frequently use to prove identification, such as drivers' licenses, birth certificates, and social security cards, are easily faked or procured fraudulently. Consequently, LPA supports efforts to enhance the credibility of documents and reduce fraud. LPA believes it is especially critical to enhance procedures used to verify identification at the time identification documents are initially issued and to use technologies that protect the integrity and security of the document.

LPA supports proposals advocated by AAMVA, which take three critical first steps in improving the integrity, reliability, and security of state-issued identification cards. Specifically, the proposals would:

- create minimum standards for identity verification that states must adopt;
- improve interoperability of state DMV databases and provide limited access to federal databases; and
- increase penalties for creating fake identification documents and additional strengthening of anti-fraud initiatives.

Setting federal minimum standards for identity verification is perhaps the most critical component of the AAMVA proposal and is strongly supported by LPA. Identification documents are only meaningful if the initial process by which they are obtained contains necessary safeguards to ensure that the recipient of the ID card is indeed the individual they claim to be. Failure to implement such safeguards has led to the situation that exists in many states today that has been characterized as the "garbage-in, garbage-out" problem. Put another way, if individuals are permitted to obtain ID documents, such as a drivers' license, by using other fraudulent documents, such as birth certificates, then the security provided by the drivers' license is minimal and of little value. Implementing federal minimum standards would go a long way toward mitigating the garbage-in, garbage-out problem by establishing a baseline below which no state could fall.

Improved access among state and federal databases will also help to improve security. In particular, by proposing implementation of the Driver Record Information Verification System, which will house information on all registered drivers and those who have had licenses revoked in the United States, states can better ensure that they are not issuing identification cards to an individual who already possesses such a card from another jurisdiction. Using such a system in conjunction with appropriate unique identifiers would further reduce opportunity for fraud.

Additionally, access to appropriate federal databases, such as immigration records, could help ensure that identification documents are only issued to those legally present in the United States and legally permitted to use those documents, a process that could be viewed as a first step at improving the employment-eligibility process.

LPA also welcomes increased penalties for those seeking to use fake documents and those that help them procure such documents. The ease by which realistic-looking

fraudulent documents can be obtained either on a street corner or over the Internet is truly disturbing. LPA recommends that states and others responsible for issuing identification documents conduct appropriate background checks, including criminal records checks, on individuals to be employed in issuing identity documents or those that will have access to facilities containing secure technology or equipment. Decreasing incentives for individuals to perpetrate such fraud and increasing audits and other programs to combat inappropriate activity by those with access to the technology and process by which legitimate IDs are made will only increase security for all as will ensuring that individuals with inappropriate backgrounds do not have access to areas where identity documents are made or processed.

Additional Steps Are Necessary to Improve Security

As noted above, improving the integrity and reliability of drivers' licenses and other forms of state issued IDs is a good first step toward improving the identification and security systems used today in the United States and any improvement in those systems will only serve to increase the general security interests of the United States. However, these aspects only address one aspect of the problem—ensuring that an individual has the identity he or she claims to have.

Yet, ensuring the integrity of identification documents only addresses part of the problem. Even if someone is who they say they are, there remains the issue of whether they have demonstrated behavioral patterns that render them inappropriate for the employment position for which they are being considered. For example, a well known failure of a background-check system in Milwaukee allowed people with criminal records to be certified for day care, including a convicted prostitute and a woman recently arrested on suspicion of beating her own daughter.[5]

Thus, much more than bolstering identification documents must be done to further increase security without inappropriately infringing on legitimate privacy interests. In particular, employers, which already play an important roll as they seek to provide safe workplaces for employees and others, should have access to those tools necessary to help them implement appropriate security policies, the implementation of which will further bolster domestic security as a whole. In particular, LPA recommends that Congress remove barriers that hinder an employer's ability to make security decisions based on an individual's complete background. The federal government should also make the creation and maintenance of accurate and timely updated databases of criminal records a priority and should permit employers to have direct access to such information to the extent it already constitutes public information.

Adequate Employer Access to Data. Employers want to provide a high level of assurance to employees, customers, clients, and the general public that they maintain safe and secure workplaces. To provide such assurances, employers often need to conduct background checks on employees, applicants, and others with access to the employer's facilities, yet there are systematic constraints that often hinder an employer's ability to do this effectively.

One common component of a comprehensive background check is a check of an individual's criminal records. Unfortunately, no central, comprehensive database exists

for checking criminal records. In fact, most states maintain criminal records at the local level and the most accurate reports may only be obtained by checking court records in individual counties. Even states that centrally collect their own county data often do not update it regularly or face technical problems that make reliance on such databases problematic.

In one recently publicized case, a Minnesota employer learned from reading a newspaper that his employee, Michael Titus, allegedly kidnapped a woman from a job site and then raped her. The employer had performed a criminal background check on the employee, searching the Minnesota Bureau of Criminal Apprehension's database of felony convictions for records of Michael C. Titus. Unfortunately, Mr. Titus's numerous convictions, which ranged from burglary to driving while intoxicated, were indexed under Michael Titus or Michael Columbus Titus, not Michael C. Titus.[6] Consequently, even though the employer thought he was searching for criminal records associated with his employee, the relevant records were not discovered until his employee had allegedly committed his crime. In addition, a later search of county court records revealed that Mr. Titus had several arrests for crimes such as aggravated assault and domestic assault that did not appear at all in the state database.[7]

But the problem of incomplete databases is by no means limited to Minnesota. Every two years the Department of Justice publishes the Survey of State Criminal History Information Systems. One of the factors examined in the last survey is whether the state database records a disposition for arrests made within the last five years (i.e., conviction, released, acquitted, etc). In 19 states, more than 40 percent of all arrest records in the past five years have no disposition whatsoever associated with them.[8]

While not as comprehensive as local databases, the federal government does maintain databases containing criminal history information, the most comprehensive of which is probably the National Crime Information Center (NCIC), which is maintained by the Federal Bureau of Investigation. However, data contained within NCIC is generally only available to law enforcement. Employers simply have no access to this data, even those components of it which are simply a compilation of public information.

Employers are sensitive to concerns that data about prospective or current employees be used prudently and in compliance with applicable laws and regulations, including guidance from the Equal Employment Opportunity Commission. At the same time, this compliance can be problematic because of a tension that sometimes exists between the myriad state and federal laws and regulations governing data access or disclosure and use of such data. This patchwork of different laws and regulations, in conjunction with the decentralized nature of data collection that exists in most of the United States today, should be kept in mind by policy makers as they seek to enact new measures to enhance security.

To address these concerns and ensure that employers can have timely access to complete background information on which to base security decisions, employers should have direct access to federal databases containing criminal history information, such as NCIC, to the extent such information is public information. Furthermore, federal, state, and local governments must take steps to ensure that information within their control is updated in a timely manner and accurate. The creation of more centralized databases,

such as on the state level rather than at the county level, would significantly help employers conduct appropriate background checks.

Legal Constraints. In ensuring employers' ability to protect their employees and the public at large, Congress also needs to reconsider some aspects of the Fair Credit Reporting Act (FCRA). While initially enacted primarily to ensure the accuracy of credit reports, FCRA also applies to employment-related background checks conducted by most third parties. FCRA imposes three principal requirements that can act as barriers to an employer seeking to base security decisions on an employee or applicant's complete record.

Specifically, the Act requires obtaining employee consent before a background check is conducted. FCRA also requires that employers disclose the content of the background check report prior to taking adverse action against the employee or applicant, and finally FCRA limits the lookback period that employers can examine in an individual's background, in most cases to seven years. In other words, employers are barred from considering most things in an employee's background that happened more than seven years ago, regardless of their relevance to determining whether the employee poses a security threat. Many states impose additional, narrower, time constraints on data an employer may collect or consider.

While it is true that some employers avoid the burdens imposed by FCRA by conducting background checks themselves, most employers find it more cost effective to use third parties who specialize in collecting such information, consequently triggering FCRA for even the most routine background investigation. LPA recommends enacting amendments to FCRA that will permit employers to consider an employee's or applicant's full record in making security decisions without undermining the fundamental privacy interests the Act seeks to address. In doing so, Congress should recall the purpose of FCRA, as codified in the law, which placed the principal emphasis on protecting the confidentiality of credit records. As enacted, FCRA specifies four key findings that the law is designed to address: fair and accurate credit reporting; elaborate systems that exist to determine creditworthiness and character of consumers; the role of reporting agencies in evaluating consumer credit and other information; and the importance of reporting agencies operating with fairness, impartiality, and a respect for the consumer's right to privacy.[9]

An additional problem imposed by FCRA involves a Federal Trade Commission opinion letter (the so-called "Vail letter") that suggested that a third party's report of an investigation into employee misconduct triggered FCRA and thus was unlawful unless obtained with the consent of the employee. As noted above, triggering FCRA would also require disclosure of the contents of the report before taking adverse action. Triggering FCRA is this context is troublesome because in the case of many investigations, such as those for sexual harassment, tipping off the employee in advance could increase risk to the victim and could thwart the investigation. In light of increased security concerns in the workplace, employers are now finding the Vail letter problematical because it hampers their ability to investigate employees who make threats and inappropriate comments and those suspected of workplace violence. The heightened security concerns we live with today make it more urgent that Congress enact a legislative fix to this

problem, such as that proposed by a bipartisan group of Members of the House of Representatives.[10]

Meanwhile, most large employers not only have their own employees working at their facilities but, at any given, a significant number of employees of their contractors are also on site. Particularly in vulnerable facilities such as power plants, chemical manufacturing plants, etc., employers want to be sure that these third parties do not pose a threat. Thus, it is critical to ensure that all personnel with access to secure areas be appropriately screened, regardless of whether they are a direct employee or a contract worker or non-traditional employee. Yet employers face substantial legal hurdles as they seek to ensure that such individuals have been appropriately screened.

To address this concern, employers may seek to have contractors conduct background checks on their employees, the contract workers. However, if the employer seeks to review those background checks to ensure that they comply with criteria the employer has established, then the contractor could be deemed to be a third party and effectively trigger FCRA. To alleviate this problem, Congress should create an exemption to FCRA for employment-related background checks either by creating a safe harbor from finding a determination of joint-employment or by clarifying that contractor employers are not acting as third party "consumer reporting agencies" when relaying background check information on contract workers to employers.

Statistical evidence underscores the importance of ensuring that employers can conduct complete and accurate background checks. As recently reported in a trade magazine, American Background Information Services reported that between January 1998 and October 2000 it found undisclosed criminal records on 12.6 percent of the individuals it screened.[11] The article reported that others found 8.3 percent of applicants to have criminal records while 23 percent misrepresented their employment or education credentials,[12] with numbers being dramatically higher in certain industries. For example, Background Check International reported that applicants in the telemarketing sector have a criminal record in 30 to 40 percent of cases.[13] Given the fact that so many applicants have criminal records or have misrepresented credentials, it is critical that employers have access to complete background information to ensure the security of the workplace.

Balancing Security with Free Flow of Commerce. Finally, the effect of new security precautions on commerce cannot be ignored. It is critical that the U.S. vigilantly protect its borders and conduct appropriate background checks on individuals seeking to enter the United States. Because trade in goods and services is critical to the economic well-being of the United States, it is important that border security procedures and protocols for granting visas be developed taking into account the importance of timely transportation of individuals and goods in commerce. LPA supports efforts to increase the integrity of passports, visas, and other travel documents to include biometrics and believes it is important for consular and immigration officials to have timely access to law enforcement, immigration, and appropriate intelligence databases. LPA also supports efforts to target resources at high-risk travelers and develop procedures to provide more timely service to pre-screened, low-risk travelers.

Conclusion

Identity documents are routinely used for many purposes in the United States, including use by employers in evaluating security risks and employment eligibility of individuals. Improvements to the integrity of commonly used identity documents, such as drivers' licenses, would significantly improve security throughout the United States. Consequently, LPA is pleased to support proposals, such as that advocated by AAMVA, that would combat fraud, establish minimum standards, and create more interoperable databases in state-issued identification cards.

However, Congress should do more to increase security nationwide by permitting employers to bolster workplace security by removing barriers that prevent employers from obtaining complete background records on which to base security decisions regarding their employees and others seeking access to the workplace. Furthermore, Congress should devote resources to improving federal, local, and state criminal databases and should provide employers with access to those databases, especially to the extent that they contain public information. Finally, as new security plans are developed, Congress should bear in mind the impact that new procedures will have on commerce and consider whether alternatives exist to mitigate the impact on commerce while maintaining a high level of security, such as by targeting resources at high-risk individuals and away from those who have been properly pre-screened and are low-risk.

Thank you for the opportunity to present testimony today on these important issues. America's employers are committed to working with you to address these and other important security issues. Please do not hesitate to call on LPA as you move forward with these proposals.

Security of the workplace is now of paramount importance to all major employers in the United States.

LPA Workplace ID Advisory Board Members

David Noznesky, Chairman
Director of Corporate Security
FPL Group Inc.

Regis W. Becker
Director, Corporate Security and Compliance
PPG Industries, Inc.

Robert Brand
Director of Corporate Security
Cox Enterprises, Inc.

David Dahl
Director, Strategic Staffing
Williams Company

Dale W. Gibbens
Director, Human Resources
Koch Industries, Inc.

Christina Ibrahim, Esq.
Counsel
Halliburton Company

Randall L. Johnson
Director, U.S. Human Resources Legislative Affairs
Motorola, Incorporated

Brian F. Keenan
Corporate Vice President, Director of Human Resources, Eastern Region
SAIC

Jeffrey Koehlinger, Esq.
Corporate Human Resources Counsel
The Dow Chemical Company

Bernard Lamoureux
Corporate Director of Security
Lockheed Martin Corporation

Barbara Landers
Managing Director, Corporate Human Resources
American Airlines Inc.

Rusine Mitchell-Sinclair
General Manager, Safety and Security Protection Services
IBM

James O'Neil
Manager, Security
United Technologies Corporation

Robert Rasor
Director of Corporate Security
General Electric Company

Thomas Ruxlow
Director of Corporate Security
Caterpillar Inc.

Julie Skipper
R&D Portfolio Manager
Eastman Kodak Company

David Smiatacz
Director, Corporate Security and Safety
Kelly Services, Incorporated

Endnotes

[1] Richard M. Stana, General Accounting Office, Illegal Aliens: Fraudulent Documents Undermining the Effectiveness of the Employment Verification System, at 2 (GAO Report HEHS-99-175, the report contains the testimony of Mr. Stana before the House Judiciary Committee's Subcommittee on Immigration and Claims on July 22, 1999).
[2] *Id.*
[3] Carol Hymowitz, *Business's New Agenda*, THE WALL STREET JOURNAL (Mar. 11, 2002) at R6.
[4] *Id.*
[5] *Blunders in Child-Care Program Intolerable*, MILWAUKEE JOURNAL SENTINEL, Jan. 16, 1998.
[6] Casey Selix, *Background Check Backfires*, SAINT PAUL PIONEER PRESS (Mar. 31, 2002).
[7] *Id.*
[8] Bureau of Justice Statistics, *Survey of State Criminal History Information Systems 1999*, at 2.
[9] 15 U.S.C. 1681(a)(1)-(4).
[10] H.R. 1543, 107th Cong., 1st Sess. (2001).
[11] Merry Mayer, *Background Checks In Focus: Thorough Screening of Recruits Can Help Prevent Surprises*, HR MAGAZINE, Jan. 2002 (available at http://www.shrm.org/hrmagazine/articles/0102/default.asp?page=0102agn-employment.asp)
[12] *Id.*
[13] *Id.*

ELECTRONIC PRIVACY INFORMATION CENTER

epic.org

April 15, 2002

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
www.epic.org

Senator Richard J. Durbin, Chairman
Subcommittee On Oversight Of Government Management,
Restructuring And The District of Columbia
332 Dirksen Senate Office Building
Washington, DC 20510
Fax: (202) 228-0400

Senator George Voinovich, Ranking Member
Subcommittee On Oversight Of Government Management,
Restructuring And The District of Columbia
317 Hart Building
Washington, DC 20510
Fax: (202) 228-1382

Re: April 16, 2002 Subcommittee Hearing on Standardizing State Driver's Licenses

Dear Senators Durbin and Voinovich,

We are writing to draw your attention to the significant opposition to the proposed establishment of a system of national identification. Enclosed is the EPIC report *Your Papers, Please: From the State Drivers License to a National Identification System*, which details the serious risk to privacy and security if proposals to standardize the state driver's license are adopted. Also enclosed is the executive summary from a new National Research Council report, *IDs--Not That Easy: Questions About Nationwide Identity Systems*, which similarly cautions against expanding the purpose of the state driver's licenses.

Recent polling data highlights the public's growing reluctance to establish a national identity system based on the state driver's license. Support for a national ID card has fallen over the last several months. A recent poll conducted by Gartner, Inc. reveals that only 26% of the population supports a card, while 41% are opposed to it. The poll also shows that the state motor vehicle departments, along with the IRS, are seen by the public to be among the least trustworthy government agencies to administer such a system if it were developed. Another poll by the Washington Post found that 44% of Americans think that a national identification card, even if it is voluntary, is "a way to keep track of people and is an invasion of people's civil liberties and privacy."

Further, a broad coalition of organizations across the political spectrum has expressed opposition to the proposal. Enclosed is the coalition letter to President Bush and Secretary Mineta encouraging them to reject proposals to create a national ID card.

Identity theft, expanded information gathering and sharing by commercial and government authorities, and the availability and use of fake or fraudulently issued driver's licenses are all significant issues that you have raised. There are a number of steps that could be taken to improve the security of the driver's license issuing system without creating a national identification system. Such steps might include better internal audits of state DMV employees and encouraging research into printing technologies that make it harder to produce fraudulent cards. The "one identity-one card" concept touted by AAMVA is the basis for a national identification scheme that will only serve to exacerbate the problem of identity theft and facilitate much greater information gathering and sharing.

Since the creation of the Social Security Number in the 1930s, the United States has remained firmly opposed to the establishment of a national ID card. Your committee is considering a serious and lasting change to America's constitutional values and tradition. We urge you to examine this proposal carefully to determine whether it is an effective response to public concerns and whether the unintended consequences have been adequately considered.

We request that this letter and its attachments be placed in the hearing record.

Sincerely yours,

Marc Rotenberg
Executive Director

Mihir Kshirsagar
IPIOP Fellow

epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

WATCHING THE WATCHERS – Policy Report #1 (February 2002)

"YOUR PAPERS, PLEASE: FROM THE STATE DRIVERS LICENSE TO A NATIONAL IDENTIFICATION SYSTEM"

An Assessment of the Proposal of the American Association of Motor Vehicle Administrators (AAMVA) to Transform the State Drivers License into a De Facto National ID Card

SUMMARY

The American Association of Motor Vehicle Administrators (AAMVA) Special Task Force on Identification Security has issued recommendations that would turn the state driver license into a de facto national ID card. The proposed scheme, analyzed in detail below, seeks federal legislation to require all states and other jurisdictions to conform to uniform standards for driver license eligibility, proof of identity, license content and document security. It would facilitate greater information sharing between jurisdictions and with state and federal agencies. It seeks to reduce fraud by encoding unique biometric identifiers on licenses and strictly enforcing prohibitions on credential fraud. But the biometric identifier would also enable new systems of identification in the private sector, and will contribute to greater profiling and surveillance of American citizens.

EPIC supports efforts to detect and prevent fraud occurring by means of the state driver's license. New technologies can reduce the risk of counterfeiting and fraud. It is also appropriate for the state Departments of Motor Vehicles (DMVs) to implement improved document security measures to prevent forgery. However, EPIC opposes AAMVA's move to standardize driver's licenses, to collect more and more invasive personal information, and to expand the information sharing capacities of DMVs.

This proposal has all the elements, risks and dangers of a national identification card system. The only distinctions between the AAMVA proposal and other National ID proposals rejected in the past are that (a) the card will not be issued by the federal government but by state motor vehicle agencies under mandatory federal regulations, and (b) the driver's license and DMV issued identity cards, held by 228 million individuals, are not (yet) mandatory. These distinctions are illusory rather than substantive, do not diminish the harm to individuals' privacy, and should not dissuade public opposition to the scheme.

The AAMVA proposal will have far-reaching and profound impacts on individual privacy. It significantly transforms the legitimate purpose of the driver's license: to certify that an individual is competent to drive a motor vehicle. It does not accomplish its stated aims of increased safety and security, but merely shifts the potential for fraud and identity theft to a higher plane, where the intrinsic privacy invasion is greater, and the means of remedying inevitable flaws in the system is more complex and difficult.

> ⇒ ***There must be wider public debate about the details and the consequences of AAMVA's national identification card and driver's license system.***

AAMVA and its industry advisors[1] have not given adequate consideration to either the details of their proposed system or its consequences. They have failed to define the scope of proper access to and use of personal information, failed to consider mechanisms to prevent internal breaches or misuse by third parties, and failed to provide a means to correct abuses when they inevitably occur.

There must be wider public debate about the details and the consequences of AAMVA's national identification card and driver's license system.

EPIC favors legislative proposals that would reduce the risks of counterfeiting and tampering, that would enable greater accuracy and reliability, and that would give individual license holders greater control over the subsequent use of their personal information. EPIC opposes provisions that would facilitate linkage of personal data among federal and state agencies, that would expand profiling of licensed drivers, and that would turn the state drivers license into an open-ended system of identification that could be routinely requested for purposes unrelated to the administration of motor vehicles and the safety of public roads.

Background of Driver's License Privacy

For more than a decade, state legislatures, the Congress, and even federal courts have worked to safeguard the privacy of driver record information. Aware that the widespread availability of the personal information obtained by state agencies for the purpose of licensing drivers has contributed to identity theft, financial loss, and even death, efforts to limit the use of driver's record information has been a high priority in the United States beginning with passage of the Drivers Privacy Protection Act of 1994, which limited the ability of state DMVs to circulate information obtained from individuals who applied for drivers licenses. The law, which was challenged by several states on federalism grounds, was upheld by the United States Supreme Court in one of the few recent opinions where the Court has held that the federal government has the authority to regulate state practices.[2]

Other steps taken to limit or reduce the risks of disclosure of personal information include efforts to allow non-commercial drivers to designate an identification number other than the Social Security Number. This change came about in part because of the awareness that the

[1] See http://www.aamva.org/links/mnu_lnkAssociate Members.asp for a list of AAMVA Associate Members & Industry Advisory Board Members and http://www.aamva.org/drivers/drvIDSecurityDocume nts.asp for a list of identification technology companies submitting reports to AAMVA's Special Task Force on Identification Security.

[2] *Condon v. Reno,* 528 U.S. 141 (2000) http://supct.law.cornell.edu/supct/html/98-1464.ZO.html. See also EPIC's Amicus Brief at http://www.epic.org/privacy/drivers/epic_dppa_brief.pdf

use of a single identifier, such as the SSN, was contributing to identity theft and white-collar crime.

States have also passed laws restricting the circumstances when a person can be required to provide a drivers license. And a federal appeals court ruled recently that it is unconstitutional for police to arrest someone for failure to provide identity documents.[3]

All of these developments in the United States over the past decade indicate widespread efforts at all levels of government to protect privacy and to reduce the risk that could result from the use of the state drivers license as a de facto national identifier.

Analysis of AAMVA recommendations[4]

Set out below is an assessment of the eight principles contained in the initial AAMVA report. The first three principles put forward by AAMVA are:

AAMVA(1) Improve and standardize initial driver's license and ID card processes
AAMVA(2) Standardize the definition of residency in all states and provinces
AAMVA(3) Establish uniform procedures for serving non-citizens

AAMVA seeks to "improve and standardize initial driver's license and ID card processes." This would include standardizing the definition of residency and imposing uniform procedures for non-citizens[5]. Such a proposal raises serious questions about the appropriate scope of state DMV authority and infringes on a state's right to develop systems and processes to serve the particular needs of its citizens.

AAMVA states its aim to "develop/capture citizenship/residence on document and/or database" within the next year.[6] It is not clear what role establishing citizenship and uniform residency status plays in the core function of a driver's license: ensuring that there are trained, safe drivers on the roads. In fact, the proposed requirements would undermine the public safety rationale of a driver's license by discouraging undocumented aliens from getting licenses, leading to more uninsured and untrained drivers on the roads and contributing to the national road toll of 40,000 deaths per year.[7] Different states have formulated specific responses to this issue based on their individual circumstances, and there is no overriding federal need to establish uniform procedures.

> ⇒ ***Centralizing authority over personal identity necessarily increases both the risk of ID theft as well as the scope of harm when ID theft occurs.***

Establishing citizenship and residency status shifts the role of the state DMVs from licensing drivers to verifying the identity of all Americans. AAMVA relies on faulty reasoning to make its argument: driver's licenses are used as identity cards for purposes unrelated to the operation of a motor vehicle, such purposes

[3] *Carey v. Nevada Gaming Control Board*, No. 00-16649 (9th Cir. 2002) http://caselaw.lp.findlaw.com/data2/circs/9th/001664 9p.pdf

[4] AAMVA Press Release, January 14 2002 [http://www.aamva.org/news/nwsPressReleaseAAM VAHelpsSecureSaferAmerica.asp].

[5] Other consequences of standardization are discussed below in the context of AAMVA's proposal for a "uniform" national driver's license.

[6] AAMVA Special Task Force on Identification Security Report to the AAMVA Board at 4 [Hereinafter "AAMVA Task Force Report"].

[7] The National Institute of Health reports 41,717 traffic fatalities in 1999. [http://www.niaaa.nih.gov/databases/crash01.txt].

include verifying employment status, opening bank accounts, and renting apartments. Since there are people who mistakenly rely on a driver's license to prove lawful status, and there are those who might seek to exploit this weakness, the appropriate solution is to change the driver license into a document that does, in fact, verify lawful presence. This is a dramatic and unwarranted expansion of function for a state *motor vehicle* department. Privacy and security interests are best protected by documents serving limited purposes and by relying on multiple and decentralized systems of identification in cases where there is a genuine need to establish identity. Centralizing authority over personal identity necessarily increases both the risk of ID theft as well as the scope of harm when ID theft occurs.

> ⇒ ***Privacy and security interests are best protected by documents serving limited purposes and by relying on multiple and decentralized systems of identification.***

AAMVA(4) Implement processes to produce a uniform, secure, and interoperable driver's license/ID card to uniquely identify an individual.

Strategy 4 is the core of AAMVA's driver license reform proposal, and contains several distinct elements that are yet to be adequately explored, developed, or discussed with the public. This strategy incorporates the following distinct ideas: uniformity (of both issuing standards and documents); security (of the identity of the applicant, and of the integrity of the document itself); interoperability (requiring uniformity, and mandating data sharing between states and with other parties); and a unique identifier.

Uniformity

AAMVA proposes that the issuing processes and requirements, as well as the information collected and maintained by the DMV, should be uniform across all states.

Uniformity of Issuing Standards

The AAMVA proposal relies upon the imposition of a national uniform standard for driver's license issuing processes.[8] AAMVA is also lobbying for Congress to delegate "the criteria and implementation of the uniform standard" to AAMVA itself.[9]

However, AAMVA have not demonstrated that uniformity is necessary to address any specified problem with the current system. They claim that "Unscrupulous individuals shop for the easiest and fastest way to get a license. They find the loopholes and they put you and me at risk."[10] There has been no substantiation from AAMVA of their claim that such "weak" licensing requirements have allowed dangerous individuals to obtain licenses, and no analysis of any security threat posed.

> ⇒ ***As yet, none of the parties involved in the proposal have announced what the new uniform processes should be.***

Further, if such a problem does exist, it can be addressed equally effectively, and without the disadvantages of a national ID system, by strengthening the issuance standards in those

[8] AAMVA Task Force Report at 2, Press Release, January 14, 2002, available at http://www.aamva.org/news/nwsPressReleaseAAMVAHelpsSecureSaferAmerica.asp

[9] Statement of Senator Durbin, Congressional Record -- Senate, S13776-13778, December 20 2001

[10] Press Release, January 14, 2002, available at http://www.aamva.org/news/nwsPressReleaseAAMVAHelpsSecureSaferAmerica.asp

states that are the "weakest links" in the system. In fact, in recent months several states have changed their application procedures to address perceived loopholes[11]. The proposal does not even demonstrate the advantages of a national uniform system over a national minimum standard, or of state-specific actions to close existing loopholes. Thus it is not narrowly tailored to the perceived problem and infringes on individual privacy for no justifiable ends.

As yet, none of the parties involved in the proposal have announced what the new uniform processes should be. It is therefore impossible to evaluate whether uniform standards would be effective in meeting perceived problems in the system, to what extent privacy interests would be compromised, and whether the proposal appropriately balances the interests of identification security and privacy.

AAMVA is not the appropriate body to be determining the balance between identification and privacy. AAMVA is a trade association that "represents the state and provincial officials in the United States and Canada who administer and enforce motor vehicle laws."[12] with a large industry advisory board including insurance, identification technology and information management companies.[13] The determination of uniform national standards and procedures is not appropriate for a bureaucracy with no direct accountability to the public, and a vested interest in the proposed system.[14] These decisions properly belongs to the state legislatures and the Congress, after a period of public debate and consultation.

Uniformity of License Documents

Just as there is no proven need for uniform application procedures and standards, there is no demonstrated need for uniformity of state driver's licenses. There are already mutual recognition programs and database pointer systems in place to address the needs AAMVA has identified. The primary reason for uniformity would be to enable information sharing with both government and private sector organizations as discussed below. In this context, uniformity intrinsically facilitates tracking, monitoring, profiling and other privacy invasive practices.

AAMVA's 90-day action plan includes efforts to "encourage voluntary short-term use of AAMVA standards in all jurisdictions," and "work with Congress to introduce DRIVerS legislation,"[15] before introducing model legislation in each AAMVA jurisdiction within one year.[16]

The adoption of the AAMVA standard by states would allow the use of driver's licenses as an identification and information gathering mechanism not only for government, law enforcement and security purposes, but also in the private sector. Products are already available that scan the AAMVA-compatible magnetic strip on a driver's license, and download 16 data fields captured on the license.[17] The information can then be compiled

[11] For example, Virginia no longer allows online renewal of driver's licenses, and has changed the identification documents required for a driver's license or identification card application: http://www.dmv.state.va.us/webdoc/citizen/drivers/applying.asp.

[12] AAMVA website http://www.aamva.org/about/

[13] AAMVA website http://www.aamva.org/links/mnu_lnkAssociateMembers.asp.

[14] AAMVAnet currently administers, and charges DMVs for access to driver and vehicle databases, and online verification networks: http://www.aamva.org/products/mnu_proAAMVANetApp.asp.

[15] AAMVA Task Force Report at 5.

[16] Id. at 3.

[17] The fields include: Last Name, First Name, Middle Name, Address1, Address2, City, State, Zip Code, Birthday, Drivers License Number, Drivers License

with data entered by the company, including a date/time stamp to track the individual's presence and information on their purchases. It may also be retained by the company, producing a database of detailed customer information that could not economically be compiled in the absence of such technology. These products are being marketed to companies that routinely check driver's licenses as identification or proof of age, including auto dealerships, clubs, bars, restaurants, and convenience stores. They are also suggested for use by health clubs and personal trainers "for use as a billing aid" and in the general retail market "to expedite adding customers to your monthly mailer."[18] AAMVA has also publicly stated that it seeks to share its model with retailers, car rental companies, insurers and banks.[19]

Security

AAMVA presents driver's license security as a single problem, but it can be distinguished into two different issues - document security and identification. EPIC supports the use of creative technology to improve document security if it is aimed at making it more difficult to counterfeit driver's licenses.[20] There is no demonstrated need, however, to establish uniform document security features across the 50 states. Each state DMV is capable of determining the needs of its customers and can incorporate features best situated to them.

Identity security concerns stem from the "one-driver, one-license, one-record" concept touted by AAMVA. In the AAMVA Special Task Force on Identification Security Report to the AAMVA Board, any pretense of a system concerned primarily with drivers is eliminated: the revised motto is "one card, one person, one record."[21] There are two main problems with such a concept. First, serving as the nation's main identity authenticators will distract a state DMV from its core function of licensing competent drivers and registering safe vehicles. Second, attempting and claiming to establish proof-positive identity is a very complex and error-prone task that creates more problems that it might solve.

Increasing reliance on the driver's license as an internal passport dramatically raises the incentives to forge or steal such credentials. If DMVs limited the use of the document for driver's licensing purposes the fraud incentives would drop significantly, particularly if the cost of fraud were raised by better document security features and stringent enforcement of identity theft laws.

> ⇒ ***As the importance of the card increases, the incentives to create fraudulent documents will also rise.***

Expiration Date, Sex, Height, Weight, Hair Color, Eye Color. See http://www.intellicheck.com/What_is_IDCheck.htm for the Intelli-Check IDCheck system, which operates not only on mag stripe cards but also 1D and 2D barcodes, and allows downloads for permanent archiving of customer identification and transaction information. See also http://www.dgahouston.com/dlsplit1.htm for product information on DLSPLIT "software to separate, format and display driver's license data," available online for US$169.60, including mag stripe reader.

[18] http://www.dgahouston.com/dlsplit1.htm for examples of "DLSPLIT Uses"

[19] "Task G: Promote the use of the Uniform Identification Practices model program developed by this Working Group to various potential customers, such as: all AAMVA jurisdictions; insurance companies, banks; travel industry; car rental agencies; retailers; others." AAMVA Uniform Identification Practices Working Group available at http://www.aamva.org/drivers/drvDL&CuniformIdentificationWG.asp

[20] Examples of such physical security features can be found listed in Appendix H of AAMVA's DL/ID Standard. Available at http://www.aamva.org/documents/stdAAMVADLIDStandrd0006630.pdf

[21] AAMVA Task Force Report at10.

DMVs must necessarily continue to rely on "breeder" documents such as birth certificates and Social Security card to establish identity. These documents are easily forged or obtained and are the main sources of identity fraud. There are currently 14,000 different versions of birth certificates in circulation.[22] A major source of fraudulent drivers licenses is DMV employees.[23] As the importance of the card increases, the incentives to create fraudulent documents will also rise. Moreover, the technology to uniquely identify individuals is untested for a large population, and previous applications of similar technology reveal significant technical error rates.[24] The enrollment process -- how we move from our current system to a unique identifier system -- will also present a number of difficult problems, including an anticipated rise in identity theft by criminals seeking to take advantage of the new procedures to establish "hardened" identities. The combination of technical concerns and prevalent American constitutional values protecting freedom of movement, privacy, and anonymity strongly suggests that any national identification scheme must be rejected.

Interoperability

For licenses to be "interoperable," they must be (a) in a compatible format across the nation, and (b) supported by a network allowing different parties to access the information linked to the individual license holder.

If AAMVA succeeded in making driver's licenses uniform across the nation (as discussed above), it would automatically satisfy the first criteria of interoperability: because there would be no relevant differences between licenses from Connecticut and Colorado, they would be interoperable.

> ⇒ ***The combination of cost, technical obstacles, and American constitutional values argue against a national identification system in the United States.***

To achieve functional interoperability, AAMVA plans to link information systems. This would enable a DMV or other authorized person to obtain the same information about a license holder regardless where the license was issued. It would also enable other entities, including government agencies and the private sector to access the information on the card. Both means of information sharing would compromise the privacy of driver's license holders.

Information sharing between states

There is already information sharing between states with regard to problem drivers in the Problem Driver Pointer System (POPS) and Commercial Drivers License System (CDLIS). There has been no demonstrated need to expand interstate information sharing beyond the existing capacity, which addresses the problems articulated thus far by AAMVA such as multiple licenses and avoidance of penalties. To the extent that AAMVA claims that PDPS does not capture problem drivers adequately, then that system should be improved, rather than creating a new system covering all drivers, including those with unblemished records.

[22] Birth Certificate Fraud (OEI-07-99-00570;9/00), September 2000, Office of Inspector General, Department of Health and Human Services, http://oig.hhs.gov/oei/reports/a492.pdf

[23] 127 California DMV employees were disciplined over the past 5 years for facilitating ID fraud. "Legislators Order DMV Audit", *Orange County Register*, February 27, 2001

[24] James L. Wayman, *Biometric Identification Standards Research, Final Report Volume I* (revision 2), San Jose State University, December, 1997 http://www.engr.sjsu.edu/biometrics/publications_fhwa.html

AAMVA's proposal for information sharing between states includes a complete feasibility study for photo exchange and specifications within 90 days.[25] But apparently regardless of the outcome of the study, AAMVA also plans to "obtain commitments for photo exchange as feasible" within the year, and begin to "implement standard image exchange" in 2003.[26]

AAMVA has set no limits on future information sharing between DMV administrators in different jurisdictions. It includes as stated goals to "coordinate effort to verify out-of-jurisdiction licenses electronically" and "continue efforts in North America *and internationally* regarding driver license/ID standards" (emphasis added).[27]

Information sharing with other entities

AAMVA has announced that it would like to link the state DMV databases with, and provide mutual access rights to, various government agencies, including SSA, INS, FBI, and some commercial organizations.

AAMVA wants its members in state DMV offices to have access to the records held by SSA, INS and Vital Statistics to assist in verifying the identity of license applicants.[28] Despite the history of abuse of personal information by DMV employees, and the privacy harm in releasing other government-held information for the unrelated purpose of driver's license ID verification, AAMVA has proposed no new safeguards to protect individuals' privacy under this practice. The AAMVA proposal to allow DMV employees to access information in state and federal agencies may require amendments to current law that protects the privacy of these records.

AAMVA has not specified the agencies that will be provided with access to driver's license information, or provided any suggested regulations to guard against a future expansion of its availability.

There is a long history of opposition by the DMVs themselves to increased information sharing, and an expansion of their information gathering function. One example of AAMVA's proposed information sharing schemes is to "improve social security number on-line verification" within one year. A similar proposal was widely rejected in 1998 under the NHTSA's Notice of Proposed Rulemaking Docket No. NHTSA-98-3945, pursuant to the (now repealed) §656(b) of the Immigration Reform Act of 1996. In a letter dated July 31 1998, opposing the NHTSA proposal, Betty Serian, Deputy Secretary of the Pennsylvania Department of Transportation, later Chair of the AAMVA Task Force on Identification Security, highlighted many of the concerns of states.[29]

Ms. Serian wrote that "the proposed requirement that states must, in all cases, verify social security numbers exceeds the statutory authority of the law" by "usurp[ing] each state's discretionary authority . . . creating a national driver's license." States require flexibility to determine what identification documents they find acceptable, based on their particular local or historical factors. Ms. Serian argued, "states

[25] AAMVA Task Force Report at 5.
[26] Id. at 3 and 5.
[27] Id. at 5.
[28] "AAMVA supports and encourages the access by its members (government entities) to other databases, such as SSA, INS and Vital Statistics to confirm identify, residency, citizenship and address verification" AAMVA Task Force Report at 8. They also plan to "improve jurisdiction access to SSA, INS and others" within a year (p. 5), "implement on-line address verification" after one year (p. 4), "continue to improve verification with the INS" within the year (p. 4)

[29] Letter on file with EPIC and available at http://www.epic.org/privacy/id_cards/penndot_letter_to_dot_ref.html.

must have the flexibility to provide for exceptions without draconian federal intervention."

Ms. Serian also cautioned of the administrative burden of the proposal, estimating that "the social security check will not match the SSA's records in approximately 20% of the cases because of the use of nicknames . . . unmarried names, data entry errors, etc. on the social security record." The SSA provides only a "Not Valid" message when the name and number do not match, forcing DMV administrators to interact with customers repeatedly. Additionally, the burden required to change data formats to achieve uniformity would be untenable. Ms. Serian stated that adding a full middle name to driver license records "would require 28 data entry clerks four years to complete the conversion" just for Pennsylvania's records. Ms. Serian concluded that the requirements were "very costly, ineffective, and customer hostile, once again adopting a theoretical approach while ignoring basic service needs of law abiding customers... Government at the state level . . . would be harmed." The additional burden in the AAMVA proposal of extra fields, including complex encoded biometric data, and altered formats to accommodate information sharing would constitute an unjustified and extravagant burden on state DMVs.

Existing Legislative Limitations on Information Sharing

Existing legislation limits the ability of DMVs and other agencies to share information. AAMVA's proposal would require substantial amendment to these laws, removing significant privacy protections that have been in place for many years.

The **Driver's Privacy Protection Act** presently contains no provisions governing the use of biometric identifiers. Before a system such as that proposed by AAMVA could come into effect, an amendment would be required incorporating biometric identifiers into the definition of "personal information" in 18 USC 2725(3),[30] and providing greater protection for the privacy of such information.

Biometric identifiers should also be incorporated in the definition of "highly restricted personal information," as defined in section 2725(4). This category currently includes "an individual's photograph or image, social security number, medical or disability information."

The prohibition on the use and disclosure of personal information in section 2721 is subject to many exceptions. The initial portion of sub-section 2721(b) requires that personal information (including highly restricted personal information) shall be disclosed in connection with the administration of a wide variety of motor vehicle related laws,[31] including

[30] 18 USC 2725(3) currently provides that "personal information" means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and the driver's status.

[31] 18 USC §2721(b): "Personal information referred to in subsection (a) shall be disclosed for use in connection with matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories, performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, and removal of non-owner records from the original owner records of motor vehicle manufacturers to carry out the purposes of titles I and IV of the Anti Car Theft Act of 1992, the Automobile Information Disclosure Act (15 USC 1231 et seq.), the Clean Air Act (42 USC 7401 et seq.), and chapters 301, 305, and 321-331 of title 49 [49 USC §§30101 et seq., 30501 et seq., 32101-33101 et seq."

environmental standards and investigation by motor vehicle manufacturers.

The prohibition on information sharing is also subject to the "permissible uses" listed in sub-section 2721(b). The permissible uses of highly restricted personal information are a subcategory of these uses, and comprise:

> (1) For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.
>
> (4) For use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.
>
> (6) For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting.
>
> (9) For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under chapter 313 of title 49 [49 USCS §§ 31301 et seq.].

Highly restricted personal information may be disclosed to any party for any with the express consent of the person to whom the information applies.[32]

There are several currently permitted uses of highly restricted personal information which would constitute further privacy violations if a biometric identifier was included on the driver's license and in the information collected by the DMVs.

The required disclosure of biometric identifiers in connection with motor vehicle laws under sub-section 2721(b) allows access to personal information by a wide variety of organizations for many purposes, where there is no demonstrated need to use such information.

The exceptions under sub-section 2721(b)(1) for sharing information with other government agencies could allow AAMVA to go even further. The provision is not limited to the SSA, INS, FBI or other agencies concerned with national security, but extends to any function of any government agency, including State and local governments and those acting on their behalf. DMV administrators thus already have the authority to share information (including biometric identifiers), and thus make provision of a driver's license a prerequisite of any interaction with government agencies.

The sensitivity of biometric information, and its use by motor vehicle administrators, was not considered by Congress at the time the Driver's Privacy Protection Act was passed in 1994.[33] The Act would require substantial amendment to take account of changes in technology, and to protect the privacy interests of driver's license holders.

[32] 18 USC §2721(a)(2).

[33] See also the discussion of biometric unique identifiers below.

There is as yet no proposal for auditing requests for access made to the DMV, or any avenue for appeal or review of decisions to grant disclosure based on the factors in the DPPA. AAMVA's proposal should include a provision requiring all DMVs to keep a record of all disclosures of personal information, and make those requests accessible to the individual to whom the information pertains.[34] If the Canadian members of AAMVA decide to join the scheme, amendments would likely be required to Canadian Provincial privacy laws, which are generally more stringent than either state or federal regulation in the United States.

Technological feasibility of information sharing

Creating a national database on 228 million Americans creates myriad problems[35]. Such a database would probably use a pointer or index system to link distinct state databases -- this is precisely how most large databases are constructed. The key issue is determining the data elements that would be used to create the index. AAMVA is lobbying for the use of the Social Security number along with name and date of birth to link the records. This is in spite of the fact that §656(b) of the Immigration Reform Act of 1996, which would have mandated the display of SSNs on state driver's license, was repealed because it would have facilitated precisely the sort of information sharing AAMVA is currently contemplating.[36]

Aside from the important policy arguments against creating such a database, these databases are notoriously mistake-prone, difficult to secure, open to abuse, and expensive to compile and operate. Reconciling different databases such as those of the Social Security Administration is expected to generate 20% error rates.[37] Linking with INS and FBI databases will likely present similar issues.

> ⇒ ***The difficulty in fixing a credit report might prove trivial in comparison to correcting one's record in the national database.***

Actually connecting the different databases is also a significant problem -- the FBI and INS have been trying to link their databases for over a decade. Moreover, large databases do not present any solution to the problem of bad data: once in a database of any sort, data -- errors and all -- tend to be authoritative, pervasive and persistent. A U.S. PIRG study found 30% of credit reports contain serious errors and 70% contain some errors.[38] The difficulty in fixing a credit report might prove trivial in comparison to correcting one's record in the national database. Instead of solving public safety problems, the government will create a bureaucratic headache that will take resources away from performing the functions that specific agencies are meant to

[34] Such a requirement exists in many state jurisdictions, often with an exception that the request information need not be provided where it relates to an ongoing criminal investigation of the person to whom the information pertains and the release would prejudice the investigation.

[35] AAMVA states that 228 million US and Canadian citizens have either a driver's license or a DMV issued identity card, representing 75 percent of the total population: AAMVA Task Force Report at 8.

[36] Report to Congress, Evaluation of Driver Licensing Information Programs and Assessment of Technologies, National Highway Traffic Safety Administration, Federal Motor Carrier Safety Administration and AAMVA, July 2001,, section 3.4.4 p. 41

[37] See Letter from Betty Serian, Deputy Secretary, Pennsylvania Department of Transportation to NHTSA, July 31, 1998 http://www.epic.org/privacy/id_cards/penndot_letter_to_dot_ref.html. See also the problems faced in California last year when the DMV began to verify social security numbers. "Glitch in DMV crackdown leaves some drivers unable to renew licenses", San Jose Mercury News, June 23, 2001

[38] Available at http://www.pirg.org/reports/consumer/mistakes/

carry out. State DMVs already operate with over-stretched resources and there is no reason why they ought to take on the burden of administering a national database.

Unique Identifier

> ⇒ ***The very attraction of biometrics for identification purposes is intrinsically linked to the infringement of individual privacy.***

AAMVA has not determined the mechanism will be used to uniquely identify individual license holders, although it has acknowledged that it contemplates the use of biometric technology. [To uniquely identify an individual, an identifier must be verifiable against the person's actual identity, that is, their permanent physical characteristics. Any alphanumeric identifier can only be verified by the possession of corresponding documents; a biometric can be used to verify the information held by the agency or on a card by reference to the actual physical characteristic it refers to. Thus it appears that AAMVA intends to implement some kind of biometric identifier.]

The very attraction of biometrics for identification purposes is intrinsically linked to the infringement of individual privacy. Whereas a license number or a PIN number can be randomly assigned, and is not in itself personally identifiable information, a biometric is inextricably linked to the particular individual it codes for. A recent opinion of the Eastern District of Pennsylvania noted that analysis of fingerprints may yield other personal information, such as the individual's environmental conditions, disease history and genetics.[39]

Notwithstanding the close link between biometrics and identity, biometrics are not fraud-proof. For example, licenses may currently be fraudulently obtained with mismatched details, such as the name, address, SSN and date of birth of one person and the photograph of another person who holds the card and may impersonate the named person. The photograph is a biometric, although not usually a digitized biometric such as AAMVA proposes, and it can be falsified. Other biometrics, such as fingerprints and retinal scans, may thus also be fraudulently placed on licenses. Their inclusion would make it extremely difficult for victims of identity theft to prove their identity, once a biometric other than theirs is associated with their driver's license.

> ⇒ ***Biometric technology is not yet sufficiently advanced to accurately identify all members of the large population of licensed drivers.***

To remedy the fact that biometric identifiers can be compromised in much the same way as the Social Security number or a photograph. AAMVA is contemplating the inclusion of multiple biometric identifiers on the license. Of course, this proposal does not make the license fraud-proof, nor change the nature of biometrics. Instead it compromises privacy and further hampers victims of identity theft with no commensurate security benefits.

Finally, biometric technology is not yet sufficiently advanced to accurately identify all members of the large population of licensed drivers. Even fingerprinting, a common technique used in law enforcement, has not been subjected to such large-scale use and there are important limitations emerging about the

[39] *USA v Llera Plaza et al*, Nos. CR 98-362-10 to 98-362-12, at 2 (E.D.P.A. filed Jan. 7, 2002) [http://www.paed.uscourts.gov/documents/opinions/02D0046P.HTM].

reliance on the technique.[40] Automated fingerprint examination is not foolproof -- a 3% error rate (a conservative guess assuming the technology and databases are used following precise directions) will mean that over 6 million Americans might be incorrectly identified in the database.[41]

For these reasons, EPIC opposes the inclusion of biometric identifiers on driver's licenses and identification cards.

AAMVA(5) Establish methods for the prevention and detection of fraud and for auditing of the driver's license/ID processes.

AAMVA(6) Ensure greater enforcement priority and enhanced penalties for credential fraud.

EPIC supports internal reform at the DMVs to remedy their record of fraud and abuse of personal information. The Driver's Privacy Protection Act provides that violations of its provisions may be addressed by individual criminal fines, per diem penalties against the DMV, and civil actions resulting in actual damages of not less than $2,500, punitive damages and costs.[42]

AAMVA have not demonstrated a need for additional laws or penalties regarding driver license fraud and unauthorized use of data. The existing laws provide strict penalties and prohibitions but AAMVA's member jurisdictions have failed to implement successful investigation and enforcement strategies. In a previous effort to combat terrorism through reducing ID fraud, the specially formulated Federal Advisory Committee on False Identification rejected the idea of a unique identifier and instead recommended better enforcement and higher penalties. These recommendations were codified in 18 USC §1028. The Internet False Identification Prevention Act of 2000 amended §1028 to address changes in technology. That Act also established a multi-agency Coordinating Committee on False Identification, which is due to report on the efficacy of current ID fraud laws in March 2002 and again in March 2003.

AAMVA(7) Seek U.S. federal and other national requirements for legislation, rule making and funding in support of AAMVA's identification and security strategies.

AAMVA proposes to "seek mandatory US federal and Canadian legislation to impose and fund national and uniform driver license/ID standards."[43] AAMVA states that such legislation would be required before any significant progress is made on its strategy. While legislative support is needed for certain key elements in the strategy, state DMVs can still move ahead on other parts without Congressional mandate. For instance, AAMVA is encouraging the voluntary use of its DL/ID standard, which facilitates information sharing among the states, enforcement authorities, and private industry.[44] AAMVA is also encouraging states to adopt uniform citizenship and residency standards as well as Social Security number verification. The problem for AAMVA is that as long as all states are not on board, the system continues to be limited. Its proposed national strategy is a way of compelling states to adopt uniform standards.

---

[40] Pankanti et al., *On the Individuality of Fingerprints* (Michigan State University 2001) http://biometrics.cse.msu.edu/cvpr230.pdf.

[41] James L. Wayman, *Biometric Identification Standards Research, Final Report Volume I* (San Jose State University December, 1997).

[42] 18 USC sects. 2721, 2723(a), 2723(b).

[43] AAMVA Task Force Report at 6.

[44] See http://www.intellicheck.com/Jurisdictions.htm for the states that have machine-readable licenses.

AAMVA must also make transparent the detailed financial structure of its program. It has asked the federal government for $100 million, however, a report from last July to Congress in which AAMVA was a co-author stated that $24 to $35 million would be required to implement an Integrated Driver License Identification System (IDLIS), with an annual operating cost of $17-$21 million.[45] The report notes that there are "substantial costs involved in developing and converting to a system encompassing all drivers" but that "once such a system would be operational, states could recover costs of operating by assessing driver license fees and related fees."[46]

AAMVA(8) Establish public and stakeholder awareness and support

It is clear that such a wide-ranging proposal requires public debate and thorough scrutiny. AAMVA's legislative schedule, as currently formulated, does not accommodate the time that would be needed for Americans to examine the appropriateness of introducing a national ID system through the state DMVs. Moreover, the technical and procedural consequences if such a scheme is implemented have not been adequately explored. At the very least, there must be a full assessment of the risks and consequences of a system of national identification in the United States. Appropriate legal and technical safeguards should be established before should a project goes forward.

⇒ There must be a full assessment of the risks and consequences of a system of national identification in the United States. Appropriate legal and technical safeguards should be established before should a project goes forward.

UNEXPECTED RESULTS

AAMVA states that it expects it national ID strategy to result in a safer America through:

a) increased security,
b) increased highway safety,
c) reduced fraud and system abuse,
d) increased efficiency and effectiveness,
e) uniformity of processes and practices.

AAMVA's scheme in fact diverts resources away from current priorities and fails to resolve any of the perceived problems. Each of its expected results is briefly refuted below:

⇒ A national ID would create a false sense of security because it would enable individuals with an ID -- who may in fact be terrorists -- to avoid heightened security measures.

Increased Security

An identity card is only as good as the information that establishes identity in the first place. Terrorists and criminals will continue to be able to obtain -- by legal and illegal means -- the documents needed to obtain a government ID, such as birth certificates and social security numbers. A national ID would create a false sense of security because it would enable individuals with an ID -- who may in fact pose security threats -- to avoid heightened security measures.

A national ID program should be evaluated in the same way we might evaluate other security countermeasures. First, what problem are IDs

[45] Report to Congress, Evaluation of Driver Licensing Information Programs and Assessment of Technologies, National Highway Traffic Safety Administration, Federal Motor Carrier Safety Administration and AAMVA, July 2001, Section 3.6 at 43

[46] Id. at 3

trying to solve? Second, how can an ID system fail to achieve its goals in practice? Third, given the failures and the loopholes in the system, how well do IDs solve the security problem? Fourth, what are the costs associated with IDs? And finally, given the effectiveness and costs, are IDs worth it?

Increased Highway Safety
Information on problem drivers is already shared between states under the Problem Driver Pointer System, administered by AAMVA. Any deficiencies in this system can be remedied by amending its scope and operation: a new system for law-abiding motorists is unnecessary. Establishing uniform residency and citizenship standards and cross-checking applications with criminal records would discourage many people from getting licenses and therefore increase the number of untrained and unlicensed drivers on the roads.

> ⇒ ***Ordinary citizens will get caught in the cracks of the new bureaucratic machinery and will have a more difficult task in remedying identity fraud and protecting privacy.***

Reduced Fraud & System Abuse / Increased Efficiency & Effectiveness
If the driver license acquires more importance in society as a "gateway" or internal passport document, the incentives for fraud will greatly increase. The unprecedented infrastructure required for creating a national ID scheme would make it difficult to differentiate abuses from technical errors and glitches. Ordinary citizens will get caught in the cracks of the new bureaucratic machinery and will have a more difficult task in remedying identity fraud and protecting privacy. The error rates alone will reduce system-wide efficiency and make the process of obtaining a driver's license a nightmare. There is no precedent for such a large database being effectively compiled and securely managed. If prior experience is any guide, the technological, privacy and security problems will be formidable.

Uniformity in Processes & Practices
There is no reason to impose uniform processes and practices, and override each state's right to develop its own practices. It will take significant resources to ensure that processes and practices are truly uniform across the country. California, for instance has been collecting fingerprints for over 20 years but most of the 60 million prints in its database are useless because of poor operating practices in collecting the data. [47] Such errors will only be magnified in a national program. Finally, AAMVA does not demonstrate how "uniformity in process and practices" is either necessary or effective in creating a "safer America."

> ⇒ ***There are several less expensive, less invasive and better-crafted alternatives***

Alternatives

There are several less expensive, less invasive and better-crafted alternatives which would not lead to the creation of a national ID card yet would address AAMVA's perceived problems of poor document security. For instance, AAMVA might develop training programs to improve the ability of DMV staff to detect fraudulent documents. Technology can be used creatively to enhance document security using features such as holograms and ultra fine lines. AAMVA can also help develop model audit and verification systems that states can choose to implement if they feel their procedures are inadequate.

[47] "Failure to finger fraud: DMV's thumbprint database is insufficient -- and costly to fix." Orange County Register, December 31, 2000

Recommendations

AAMVA's proposal to implement a national ID scheme through the driver's license system is a backward step for individual privacy with no substantial countervailing safety or security benefits. At present, the case against adoption of a national ID card in the United States is compelling.

- Efforts to detect and prevent fraud occurring within DMVs, or with the assistance of DMVs and their employees, should be pursued.

- Improved document security measures to prevent counterfeiting and tampering are overdue and should be pursued, but measures that enable profiling and tracking of licensed drivers in the United States raise far-reaching policy concerns.

- AAMVA's move to standardize driver's licenses nationally, to collect more and more invasive personal information, and to expand the information sharing capacity of DMVs raises substantial privacy concerns that have not been adequately addressed

- AAMVA's proposal has all the elements and problems of a National ID Card. Although the card would not be mandated by federal law or issued by a federal agency, in many respects it reaches further than a simple ID card and might be better understood as the creation of a National Identification System. AAMVA recognizes this, citing as a "major implication" of their proposal that "the continued evolution and improvements of the driver license/ID card precludes the need for a new, separate national identification card."[48]

- AAMVA's proposal significantly changes the purpose of the driver's license: to certify that an individual is competent to drive a motor vehicle. In diluting this central function, the AAMVA proposal may reduce public safety.

- The increasing reliance on a single centralized form of identification makes ID theft simpler, and more difficult for victims to remedy.

- AAMVA must define the scope of proper access to and use of personal information, consider mechanisms to prevent internal breaches or misuse by third parties, and provide a means to correct abuses when they inevitably occur, before its proposal can be thoroughly analyzed.

- There must be wider public debate about the details and the consequences of AAMVA's national identification card and driver's license system. This proposal is moving too quickly, with too little consideration of the long-term impact on privacy and the risk of new forms of identity theft and fraud.

CONCLUSION

The combination of technical concerns and prevalent American constitutional values protecting freedom of movement, privacy, and anonymity strongly suggests that any national identification scheme must be rejected.

REFERENCES

AAMVA website: http://www.aamva.org

AAMVA Driver's License / Identification Card Standard
http://www.aamva.org/standards/stdAAMVADLIdStandard2000.asp (summary)

[48] AAMVA Task Force Report at10.

http://www.aamva.org/Documents/stdAAMVADLIDStandrd000630.pdf (full report)

AAMVA Executive Committee Resolution establishing the Special Task Force on Identification Security
http://www.aamva.org/Documents/hmExecResolution.pdf

AAMVA Special Task Force on Identification Security information
http://www.aamva.org/drivers/drvIDSecurityindex.asp

AAMVA Special Task Force on Identification Security Report to the AAMVA Board, Executive Summary
http://www.aamva.org/drivers/drvIDSecurityExecutiveSummary.asp. (Full report on file with EPIC).

Commercial Applications of AAMVA Standard Driver's Licenses:
http://www.dgahouston.com/dlsplit1.htm
http://www.intellicheck.com/

Driver's Privacy Protection Act 18 USC §2721 et seq.

Statement of Senator Richard Durbin, Congressional Record -- Senate, S13776-13778, December 20 2001

Letter from Betty Serian, Deputy Secretary, Pennsylvania Department of Transportation to NHTSA dated July 31 1998
http://www.epic.org/privacy/id_cards/penndot_letter_to_dot_ref.html

USA v Llera Plaza et al, Nos. CR 98-362-10 to 98-362-12 (E.D.P.A. filed Jan. 7, 2002) (motion to preclude the US from introducing latent fingerprint identification evidence)
http://www.paed.uscourts.gov/documents/opinions/02D0046P.HTM

Condon v. Reno, 528 U.S. 141 (2000).
http://supct.law.cornell.edu/supct/html/98-1464.ZO.html

Carey v. Nevada Gaming Control Board, No. 00-16649 (9th Cir. 2002)
http://caselaw.lp.findlaw.com/data2/circs/9th/0016649p.pdf.

Reports

James L. Wayman, *Biometric Identification Standards Research, Final Report Volume* I, San Jose State University December, 1997
http://www.engr.sjsu.edu/biometrics/publicatios_fhwa.html

Office of Inspector General, Department of Health and Human Services. *Birth Certificate Fraud*, September 2000
http://oig.hhs.gov/oei/reports/a492.pdf

John J. Miller and Stephen Moore, *A National Id System: Big Brother's Solution to Illegal Immigration*, September 7, 1995
http://www.cato.org/pubs/pas/pa237es.html

Sharath Pankanti, Salil Prabhakar & Anil K. Jain, *On the Individuality of Fingerprints*, Michigan State University, 2001
http://biometrics.cse.msu.edu/cvpr230.pdf

Public Interest Research Group (PIRG), *Mistakes Do Happen: Credit Report Errors Mean Consumers Lose*, March 1998
http://www.pirg.org/reports/consumer/mistakes/

National Highway Traffic Safety Administration, Federal Motor Carrier Safety Administration and AAMVA, *Report to Congress, Evaluation of Driver Licensing Information Programs and Assessment of Technologies*, July 2001

http://www.aamva.org/Documents/Library/libNHTSAReportToCongress.pdf

Robert Ellis Smith, *A National ID Card: A License to Live, Privacy Journal,* December 2000.

Shane Ham and Robert D. Atkinson, *Modernizing the State Identification System: An Action Agenda*, February 2, 2002 http://www.ppionline.org/documents/Smart_Ids_Feb_02.pdf

Charlotte Twight, *Why Not Implant a Microchip?*, February 7, 2002 http://www.cato.org/dailys/02-07-02.html

Adam Thierer, *National ID Cards: New Technologies, Same Bad Idea*, TechKnowledge No. 21, September 28, 2001 http://www.cato.org/tech/tk/010928-tk.html

Lucas Mast, *Biometrics: Hold On, Chicken Little*, TechKnowledge No. 31, January 18, 2002 http://www.cato.org/tech/tk/020118-tk.html

Simon G. Davies, "Touching Big Brother: How biometric technology will fuse flesh and machine," *Information Technology & People,* Vol 7, No. 4 1994. http://www.privacy.org/pi/reports/biometric.htl

EPIC ID Card Resource Page http://www.epic.org/privacy/id_cards/

ABOUT EPIC

The Electronic Privacy Information Center is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, freedom of expression and constitutional values in the information age. EPIC pursues a wide range of activities, including policy research, public education, conferences, litigation, publications, and advocacy. The Watching the Watchers Project was undertaken by EPIC in 2001 to assess the impact of proposals for public surveillance put forward after September 11.

Lycos Home | Site Map | My Lycos | Lycos Mail

WIRED NEWS BUSINESS POLITICS WIRE SERVICE CULTURE TECHNOLOGY TOP STORIES

Support for ID Cards Waning

By Julia Scheeres

2:00 a.m. March 13, 2002 PST

Support for a national ID card, which hit an all-time high after the Sept. 11 attacks, appears to be fading, according to a nationwide poll released Tuesday.

A survey by Gartner Inc. found that 41 percent of Americans opposed a national identification system, while 26 percent backed the idea.

See also:

- DMVs Pushing for Standard License
- Oracle Keeps Pushing ID Card
- The Oracle of National ID Cards
- ID Cards Are *de Rigueur* Worldwide
- Keep an eye on Privacy Matters
- Conflict 2001: Fresh Perspectives

The results contrast sharply with a Pew Research Center poll conducted the week after the attack, in which 70 percent of respondents supported a national ID card that would be shown to authorities on demand.

The Gartner poll, which queried 1,120 people by phone and probed the issue deeper than previous questionnaires, found that respondents' endorsement of a national ID system varied according to their perception of how it would be used. Respondents supported the airlines use of such a database to verify passengers' identities, for example, but balked at the idea of needing a national ID card to access bank and health care services.

Richard Hunter, a vice president for security research at Gartner, said the results reflected growing fears about potential abuse of the system.

"Our data shows that people would only support a national ID for very specific, very limited purposes and that they're suspicious of what government agencies will do with their information," Hunter said.

The survey also found that respondents preferred that private industries -- such as bank or credit card companies -- administer the system and not governmental bodies. (Among government agencies, respondents said they'd pick the FBI to do the job if they had to make a choice.)

Calls for a national ID system cropped up after it was revealed that at least 11 of the Sept. 11 hijackers had used false identities. But enthusiasm for what some people have categorized as a knee-jerk reaction to the attacks has waned as privacy concerns emerge.

"I really think decreased support is linked to better awareness," said Mihir Kshirsagar, a policy fellow at the Electronic Privacy Information Center (EPIC). "Not only does it fly in the face of prevailing constitutional values and principles, it has very little to do with combating terrorism."

ID cards won't thwart future terrorist attacks, he said, because the criminals will still be able to purchase fraudulent documents, such as birth certificates, that would be needed to obtain the IDs. Privacy advocates also fear that the cards themselves would act as a kind of national passport, allowing authorities to monitor people's movements and activities.

EPIC and other groups believe that increased information-sharing among government agencies is just as insidious as having to fork over your ID card to cops who think you look "suspicious."

Officials' abuse of databases filled with private citizen information has been well documented. Take the recent case of Emilio Calatayud. The 12-year DEA veteran is charged with selling criminal histories pulled from a law enforcement database to a private investigative firm in Los Angeles over the course of six years before getting caught.

Related Wired Links:

Spying: The American Way of Life?
March 11, 2002

They Want Their ID Chips Now
Feb. 6, 2002

The Oracle of National ID Cards
Oct. 27, 2001

Congress Weighs Anti-Terror Bill
Sep. 25, 2001

ID Cards Are *de Rigueur* Worldwide
Sep. 25, 2001

Copyright © 1994-2002 Wired Digital Inc. All rights reserved.

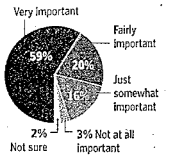
» **Lycos Worldwide** © Copyright 2002, Lycos, Inc. All Rights Reserved. Lycos® is a registered trademark of Carnegie Mellon University.
About Terra Lycos | Help | Feedback | Jobs | Advertise | Business Development
Your use of this website constitutes acceptance of the Lycos Network Privacy Policy and Terms & Conditions

THE FEDERAL PAGE
WEDNESDAY, FEBRUARY 27, 2002 A21

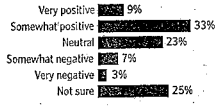
E-Government Poll

Many Americans believe e-government—federal, state or local government services and communications online—"has a critical role to play" in the war against terrorism, according to a report released yesterday by the Council for Excellence in Government. The council said a poll conducted for the group by the research firms of Peter D. Hart and Robert M. Teeter showed that a large majority of the public, for example, believes e-government will help federal and local agencies better coordinate a response to an emergency. The poll also indicates that many Americans have mixed feelings about national identification cards, are concerned about online security and believe that e-government can improve government accountability. Hart-Teeter conducted the telephone survey of 961 randomly selected adults from Nov. 12 to Nov. 19.

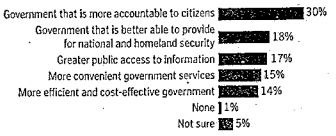
Q. How important is it to you that government invest in e-government that improves communication between government agencies and federal, state, and local governments so that government is better able to protect our national and homeland security?



Q. Would you say e-government is having a very positive, somewhat positive, neutral, somewhat negative or very negative effect on the way that government operates?



Q. I'm going to read you a list of positive things that may result from e-government. Which one do you think would be the most important?



Q. Which one comes closer to your own opinion?

The national identification card would make electronic transactions with the government and business faster and more secure for people, and using the card would be an easier way for people to verify their identity in places such as airports and government offices. **47%** chose this option

The national identification card is a way to keep track of people and is an invasion of people's civil liberties and privacy. Although the card is voluntary, it would make it more difficult for people who chose not to get the card to prove their identity and make transactions. **44%** chose this option

THE WASHINGTON POST

ELECTRONIC PRIVACY INFORMATION CENTER

BY FAX AND MAIL

February 11, 2002

President George W. Bush
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Dear President Bush:

We, representing a broad and diverse coalition of national organizations, urge the Administration to oppose the attempts of state motor vehicle officials to create a national identification system (national ID) through the bureaucratic back door of state drivers' licenses.

One reaction to the terrible events of September 11 was renewed discussion about instituting a national ID card as a counter-terrorism measure. The creation of a national ID card or system is a misplaced, superficial "quick fix" to the terrorist threat. A national ID system would not effectively deter terrorists and, instead, would pose serious threats to the rights of freedom and equality of everyone in the United States.

Although national ID proposals received fierce debate in the fall, the Administration and Congress wisely rejected them. Direct passage of a national ID card, however, is only one possible path to such a system. A national ID would more likely evolve bureaucratically through existing forms of ID, such as state drivers' licenses.

The American Association of Motor Vehicle Administrators (AAMVA) is urging the federal government to fund and authorize a proposal to standardize state drivers' licenses. This plan would establish a national ID and an unparalleled system of personal information sharing.

We urge you to reject this proposal because:

A national ID would not prevent terrorism. An identity card is only as good as the information that establishes identity in the first place. Terrorists and criminals will continue to be able to obtain – by legal and illegal means – the documents needed to get a government ID, such as birth certificates and social security numbers. A national ID would create a false sense of security because it would enable individuals with an ID – who may in fact be terrorists – to avoid heightened security measures.

A national ID would depend on a massive bureaucracy that would limit our basic freedoms. A national ID system would depend on both the issuance of an ID card and the integration of huge amounts of personal information included in state and federal government databases. One employee mistake, an underlying database

error rate, or common fraud could take away an individual's ability to move freely from place to place or even make them unemployable until the government fixed their "file." Anyone who has attempted to fix errors in their credit report can imagine the difficulty of causing an over-extended government agency such as the department of motor vehicles to correct a mistake that precludes a person from getting a valid ID.

A national ID would be expensive and direct resources away from other more effective counterterrorism measures. The costs of a national ID system have been estimated at as much as $9 billion. Even more troubling, a national ID system mandated through state agencies would burden states who may have more effective ways to fight terrorism and strengthen ID systems.

A national ID would both contribute to identity fraud and make it more difficult to remedy. Americans have consistently rejected the idea of a national ID and limited the uses of data collected by the government. In the 1970s, both the Nixon and Carter Administrations rejected the use of social security numbers as a uniform identifier because of privacy concerns. A national ID would be "one stop shopping" for perpetrators of identity theft who usually use social security numbers and birth certificates for false IDs (not drivers' licenses). Even with a biometric identifier, such as a fingerprint, on each and every ID, there is no guarantee that individuals won't be identified - or misidentified - in error. The accuracy of biometric technology varies depending on the type and implementation. And, it would be even more difficult to remedy identity fraud when a thief has a National ID card with your name on it, but his biometric identifier.

A national ID could require all Americans to carry an internal passport at all times, compromising our privacy, limiting our freedom, and exposing us to unfair discrimination based on national origin or religion. Once government databases are integrated through a uniform ID, access to and uses of sensitive personal information would inevitably expand. Law enforcement, tax collectors, and other government agencies would want use of the data. Employers, landlords, insurers, credit agencies, mortgage brokers, direct mailers, private investigators, civil litigants, and a long list of other private parties would also begin using the ID and even the database, further eroding the privacy that Americans rightly expect in their personal lives. It would take us even further toward a surveillance society that would significantly diminish the freedom and privacy of law-abiding people in the United States. A national ID would foster new forms of discrimination and harassment. The ID could be used to stop, question, or challenge anyone perceived as looking or sounding "foreign" or individuals of a certain religious affiliation.

The Fiscal Year 2002 House Transportation Appropriations' report encourages the Department to study and define "the types of encoded data that should be placed on drivers' licenses for security purposes, and to work in concert with the states toward early implementation of such measures." These guidelines could be the first step toward federal involvement in the standardization of state drivers' licenses and the implementation of a national ID. We urge you to make recommendations that would provide the states with a series of security options rather than one uniform standard that could lead to a national ID.

We urge the Administration to reject national ID systems in any form. The Administration should not take any steps to implement such a system or fund any proposals that would result in a national ID, including the study or development of standardized state drivers' licenses.

There are more effective methods to prevent terrorism that would not impact the liberty interests of Americans.

We would appreciate the opportunity to meet with you to discuss these issues in more detail. Please contact Lori Waters at the Eagle Forum, (202) 544-0353; Katie Corrigan at the American Civil Liberties Union, (202) 675-2322; Brad Jansen at Free Congress Foundation, (202) 546-3000; or Chris Hoofnagle at the Electronic Privacy Information Center, (202) 483-1140.

Sincerely,

American-Arab Anti-Discrimination Committee
American Civil Liberties Union
American Conservative Union
American Immigration Lawyers Association
American Legislative Exchange Council
American Policy Center
Americans for Tax Reform
Arab American Institute
Center for Democracy and Technology
Citizens Committee for the Right to Keep and Bear Arms
Citizens' Council on Health Care
Coalitions for America
Common Ground
Consumer Alert
Consumers Against Supermarket Privacy Invasion and Numbering
Council on American Islamic Relations
Eagle Forum
Electronic Frontier Foundation (Joined Feb. 12, 2002)
Electronic Privacy Information Center
Free Congress Foundation
Friends Committee on National Legislation (Quaker)
God Bless America
Home School Legal Defense Association
Independent Institute
Japanese American Citizens League
Leadership Conference on Civil Rights
Libertarian Party
Liberty Counsel
Life Coalition International
Mexican American Legal Defense and Educational Fund
Multiracial Activist and Abolitionist Examiner
National Asian Pacific American Legal Consortium
National Conference of State Legislatures

National Consumers League
National Council of La Raza
National Vaccine Information Center
Organization of Chinese Americans
Parents Requesting Open Vaccine Education
People Against Church Taxation
People for the American Way
Privacilla.org
Privacy International
Privacy Rights Clearinghouse

cc:
United States House of Representatives
United States Senate

http://www.nap.edu/openbook/030908430X/html/R1.html, copyright , 2001 The National Academy of Sciences, all rights reserved

IDs—Not That Easy
Questions About Nationwide Identity Systems

Stephen T. Kent and Lynette I. Millett, *Editors*

Committee on Authentication Technologies and Their Privacy Implications

Computer Science and Telecommunications Board

Division on Engineering and Physical Sciences

National Research Council

NATIONAL ACADEMY PRESS
Washington, D.C.

http://www.nap.edu/openbook/0309083038/html/R2.html, copyright © 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

NOTICE: The project from which this report was generated was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

Support for this project was provided by the National Science Foundation, the Office of Naval Research, the General Services Administration, the Federal Chief Information Officers' Council, and the Social Security Administration. Support for this special report was provided by theVadasz Family Foundation, a contributor to the Computer Science and Telecommunications Board's program on information technology and society.' Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the sponsors.

Library of Congress Catalog Card Number **xxx**
International Standard Book Number **xxx**

Additional copies of this report are available from:

National Academy Press
2101 Constitution Avenue, NW
Box 285
Washington, DC 20055
800/624-6242
202/334-3313 (in the Washington metropolitan area)

The report is also available online at http://www.nap.edu or http://www.cstb.org/

Copyright 2002 by the National Academy of Sciences. All rights reserved.
Printed in the United States of America.

http://www.nap.edu/openbook/0309084830/html/iii.html copyright 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

THE NATIONAL ACADEMIES

National Academy of Sciences
National Academy of Engineering
Institute of Medicine
National Research Council

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Bruce M. Alberts is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Wm. A. Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Kenneth I. Shine is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Bruce M. Alberts and Dr. Wm. A. Wulf are chairman and vice chairman, respectively, of the National Research Council.

http://www.nap.edu/openbook/0309084,08X/html/R4.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

COMMITTEE ON AUTHENTICATION TECHNOLOGIES AND THEIR PRIVACY IMPLICATIONS

STEPHEN T. KENT, BBN Technologies, *Chair*
MICHAEL ANGELO, Compaq Computer Corporation
STEVEN BELLOVIN, AT&T Labs Research
BOB BLAKLEY, IBM Tivoli Software
DREW DEAN, SRI International
BARBARA FOX, Microsoft Corporation
STEPHEN H. HOLDEN, University of Maryland at Baltimore County
DEIRDRE MULLIGAN, University of California at Berkeley
JUDITH S. OLSON, University of Michigan
JOE PATO, HP Labs Cambridge
RADIA PERLMAN, Sun Microsystems
PRISCILLA M. REGAN, George Mason University
JEFFREY SCHILLER, Massachusetts Institute of Technology
SOUMITRA SENGUPTA, Columbia University
JAMES WAYMAN, San Jose State University
DANIEL J. WEITZNER, Massachusetts Institute of Technology

Staff

LYNETTE I. MILLETT, Study Director and Program Officer
JENNIFER BISHOP, Senior Project Assistant (beginning October 2001)

http://www.nap.edu/openbook/0309084330/html/R5.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD

DAVID D. CLARK, Massachusetts Institute of Technology, *Chair*
DAVID BORTH, Motorola Labs
JAMES CHIDDIX, AOL Time Warner
JOHN M. CIOFFI, Stanford University
ELAINE COHEN, University of Utah
W. BRUCE CROFT, University of Massachusetts at Amherst
THOMAS E. DARCIE, AT&T Labs Research
JOSEPH FARRELL, University of California at Berkeley
JEFFREY M. JAFFE, Bell Laboratories, Lucent Technologies
ANNA KARLIN, University of Washington
BUTLER W. LAMPSON, Microsoft Corporation
EDWARD D. LAZOWSKA, University of Washington
DAVID LIDDLE, U.S. Venture Partners
TOM M. MITCHELL, Carnegie Mellon University
DONALD NORMAN, Nielsen Norman Group
DAVID A. PATTERSON, University of California at Berkeley
HENRY (HANK) PERRITT, Chicago-Kent College of Law
BURTON SMITH, Cray Inc.
TERRY SMITH, University of California at Santa Barbara
LEE SPROULL, New York University
JEANNETTE M. WING, Carnegie Mellon University

MARJORY S. BLUMENTHAL, Director
HERBERT S. LIN, Senior Scientist
ALAN S. INOUYE, Senior Program Officer
JON EISENBERG, Senior Program Officer
LYNETTE I. MILLETT, Program Officer
CYNTHIA A. PATTERSON, Program Officer
STEVEN WOO, Program Officer
JANET BRISCOE, Administrative Officer
DAVID PADGHAM, Research Associate
MARGARET HUYNH, Senior Project Assistant
DAVID DRAKE, Senior Project Assistant
JANICE SABUDA, Senior Project Assistant
JENNIFER M. BISHOP, Senior Project Assistant
BRANDYE WILLIAMS, Staff Assistant

For more information on CSTB, see its Web site at <http://www.cstb.org>, write to CSTB, National Research Council, 2101 Constitution Avenue, N.W., Room HA 560, Washington, DC 20418, call at (202) 334-2605, or e-mail the CSTB at cstb@nas.edu.

http://www.nap.edu/openbook/0309088348/html/R7.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

Preface

The terrorist attacks of September 11, 2001, and subsequent discussions have brought fresh urgency to the challenges of providing information security. In the wake of these and other recent events, numerous proposals have been circulating both in policy circles and the national media.

One proposal that has received a fair amount of attention is a national identification card—or, more precisely, a nationwide identity system. The Bush administration has indicated that a national identification card is not within the scope of options it is contemplating. Congress, however, has been considering various alternatives, for example, a measure in the USA-PATRIOT Act would "require foreigners to use identification cards to enter the United States," and other bills propose centralized national databases for visa holders and other noncitizens. Additional suggestions include a proposal by the American Association of Motor Vehicle Administrators (AAMVA) to link state motor vehicle departments and a proposed "trusted traveler" system for airports.

The persistence of public discussion on the topic and the expectation that other proposals will be offered argue for an informed analysis and critique of the concept of a nationwide identity system.

In early 2001, the Computer Science and Telecommunications Board, a unit of the National Research Council with a long history of examining information technology, security, and related issues,[1] launched a study to examine authentication technologies and their privacy implications. Sponsored by the National Science Foundation, the Office of Naval Research, the General Services Administration, the Federal Chief Information Officers' Council, and the Social Security Administration, the study aims to assess emerging approaches to user authentication in computing and communications systems, and it specifically focuses on the implications of these authentication technologies for privacy.

The study is being conducted by the multidisciplinary Committee on Authentication Technologies and Their Privacy Implications whose members include experts in the design, implementation, deployment, and use of information systems generally and information systems security in particular, along with experts in privacy law and policy (see Appendix A for Committee and Staff biographies). Given that identification and authentication systems constitute a large portion of the committee's agenda, it is well positioned to comment on technology and policy issues surrounding a nationwide identity system and its supporting infrastructures (hereinafter referred to as a nationwide identity system). In fact, CSTB asked the committee to do so, in the interest of providing a timely contribution to the public debate. Additional resources from the Vadasz Family Foundation enabled development of this report.

The committee's broader and more comprehensive final report is expected in late 2002, but its members felt compelled to issue a brief report at this time because of the real possibility that further debate on a nationwide identity system, and even action on the topic, could take place prior to the final report's issuance. Thus the present effort outlines the issues the committee believes must be addressed and raises a number of questions that the committee believes should be answered as part of any consideration of a nationwide identity system.

[1] See, for example, CSTB reports such as *Growing Vulnerability of the Public Switched Networks* (1989), *Computers at Risk* (1991), *Evolving the High Performance Computing and Communications Initiative to Support the Nation's Information Infrastructure* (1995), *Cryptography's Role in Securing the Information Society* (1996), *For the Record: Protecting Electronic Health Information* (1997), *Trust in Cyberspace* (1999), *The Internet's Coming of Age* (2000), *Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers* (2001), and *Cybersecurity Today and Tomorrow: Pay Now or Pay Later* (2002). See <http://www.cstb.org/web/topic_security> for a complete list of CSTB reports related to security, assurance, and privacy.

http://www.nap.edu/openbook/0309084830/html/R8.html, copyright , 2001 The National Academy of Sciences, all rights reserved

This brief report is a product of the committee's deliberations, drawing on its members' areas of expertise. But, given time and resource limitations, it is not an exhaustive assessment. It is intended to catalyze a broader and more sophisticated discussion. Clearly, the legal, policy, and technological issues associated with nationwide identity systems warrant a much more detailed and comprehensive examination. The committee invites feedback on this brief report as it continues the process of preparing its broader and more in-depth final report on the topic of authentication technologies and their implications for privacy.

The committee thanks David D. Clark, chair of the CSTB, and Marjory S. Blumenthal, CSTB's director, for their commentary and feedback on draft versions of the report. The committee also wishes to thank the various members of the CSTB staff who helped to make it happen. Jennifer Bishop took over as senior project assistant for the authentication study midway through the project, managing logistics, organizing materials, and coping with an unplanned brief report and review with aplomb. She also assisted in developing the diagrams in the report and designed its cover. Janet Briscoe, CSTB's administrative officer, provided crucial administrative, and logistical support as well as the suggestion that ultimately led to the report's title. Andy White, director of the NRC's Committee on National Statistics, provided feedback during the formulation and review phases. The committee also thanks Steven J. Marcus, a freelance editor, for assistance at multiple stages of the report's development. Liz Fikre at the National Research Council also made significant editorial contributions to the final manuscript. Lynette Millett is the study director for this project; she synthesized this report, coordinating contributions from committee members and drafting the response to reviewers.

Stephen T. Kent, Chair
Committee on Authentication Technologies and Their Privacy Implications

http://www.nap.edu/openbook/0309084393/html/R9.html, Copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

Acknowledgment of Reviewers

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report:

Alfred Blumstein, Carnegie Mellon University
Michael Caloyannides, Mitretek Systems, Inc.
Julie E. Cohen, Georgetown University Law Center
Jerome H. Saltzer, Massachusetts Institute of Technology
Peter Swire, George Washington University
Lee M. Zeichner, LegalNet Works, Inc.

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations, nor did they see the final draft of the report before its release. The review of this report was overseen by Willis Ware of RAND. Appointed by the National Research Council, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

http://www.nap.edu/openbook/0309084030/html/R11.html. copyright , 2001 The National Academy of Sciences. all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

Contents

EXECUTIVE SUMMARY 1

1 INTRODUCTION AND OVERVIEW 3

WHAT DOES IDENTITY PROVIDE? 13
TO WHOM AND FOR WHAT? 15
PERMITTED USERS OF THE SYSTEM 17
PERMITTED USES OF THE SYSTEM 19
VOLUNTARY OR MANDATORY? 20
WHAT LEGAL STRUCTURES? 21
BENEFITS AND DRAWBACKS 21

3 TECHNOLOGICAL CHALLENGES 25

BINDING PERSONS TO IDENTITIES 27
BACKEND SYSTEMS 28
DATA CORRELATION AND PRIVACY 30

4 CONCLUDING REMARKS 35

APPENDIXES 37

A COMMITTEE MEMBER AND STAFF BIOGRAPHIES 37
B WHAT IS CSTB? 43

http://www.nap.edu/openbook/0309084.0X/html/R12.html, copyright © 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

[PAGE INTENTIONALLY LEFT BLANK]

http://www.nap.edu/openbook/0309084032/html/1.html, copyright 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

Executive Summary

Nationwide identity systems have been proposed as a solution for problems from counterterrorism to fraud detection to enabling electoral reforms. In the wake of September 11, 2001, and renewed interest in the topic, the Committee on Authentication Technologies and Their Privacy Implications of the Computer Science and Telecommunications Board[1] developed this short report as part of its ongoing study process, in order to raise questions and catalyze a broader debate about such systems. The committee believes that serious and sustained analysis and discussion of the complex constellation of issues presented by nationwide identity systems are needed. Understanding the goals of such a system is a primary consideration. Indeed, before any decisions can be made about *whether* to attempt some kind of nationwide identity system, the question of *what* is being discussed (and why) must be answered.

There are numerous questions about the desirability and feasibility of a nationwide identity system. This report does not attempt to answer these questions comprehensively and does not propose moving towards such a system or backing away. Instead, it aims to highlight some of the significant and challenging policy, procedural, and technological issues presented by such a system, with the goal of fostering a broad, deliberate, and sophisticated discussion among policymakers and stakeholders about whether such a system is desirable or feasible.

Policy questions that the committee believes should be considered when contemplating any kind of identity system include the following:

- What is the *purpose of the system*? Possibilities range from expediting and/or tracking travel to prospectively monitoring individuals' activities in order to identify and look for suspicious activity to retrospectively identifying perpetrators of crimes.
- What is the *scope of the population* that would be issued an "ID" and, presumably, be recorded in the system? How would the identities of these individuals be authenticated?
- What is the *scope of the data* that would be gathered about individuals participating in the system and correlated with their national identity? While colloquially it is referred to as an "identification system," implying that all the system would do is identify individuals, many proposals talk about the ID as a key to a much larger collection of data. Would these data be identity data only (and what is meant by identity data)? Or would other data be collected, stored, and/or analyzed as well? With what confidence would the accuracy and quality of this data be established and subsequently determined?
- *Who would be the user(s)* of the system (as opposed to those who would participate in the system by having an ID)? One assumption seems to be that the public sector/government will be the primary user, but what parts of the government, in what contexts, and with what constraints? In what setting(s) in the public sphere would such a system be used? Would state and local governments have access to the system? Would the private sector be allowed to use the system? What entities within the government or private sector would be allowed to use the system? Who could contribute, view, and/or edit data in the system?
- What *types of use* would be allowed? Who would be able to ask for an ID, and under what circumstances? Assuming that there are datasets associated with an individual's identity, what types of queries would be permitted (e.g., "Is this person allowed to travel?" "Does this person have a criminal record?") Beyond simple queries, would analysis and data mining of the information collected be permitted? If so, who would be allowed to do such analysis and for what purpose(s)?

[1] See <http://www.cstb.org/web/project_authentication>.

http://www.nap.edu/openbook/0309084393/html/2.html, copyright , 2001 The National Academy of Sciences, all rights reserved

- Would participation in and/or identification by the system be *voluntary or mandatory*? In addition, would participants have to be aware of or consent to having their IDs checked (as opposed to, for example, allowing surreptitious facial recognition)?
- What *legal structures* protect the system's integrity as well as the data subject's privacy and due process rights, and determine the government and relying parties' liability for system misuse or failure?

Each of these issues is elaborated on in the report. And each of the above questions evokes a larger set of issues and questions that must be resolved. In addition, many of these issues are interdependent, and choices made for each will bear on the options available for resolving other issues.

Decisions made at this level will also have ramifications for the technological underpinnings of the system, including what levels and kinds of system security will be required. In fact, "system" may be the most important (and heretofore least discussed) aspect of the term "nationwide identity system," because it implies the linking together of many social, legal, and technological components in complex and interdependent ways. The success or failure of such a system is dependent not just on the individual components but also on the ways they work—or do not work—together. The control of these interdependencies, and the mitigation of security vulnerabilities and their unintended consequences, would determine the overall effectiveness of the system.

The committee believes that given the complexity and potential impact of nationwide identity systems, more analysis is needed with respect to both desirability and feasibility. In particular,

- Given the potential economic costs, significant design and implementation challenges, and risks to both security and privacy, there should be broad agreement on what problem(s) a nationwide identity system would address. Once there is agreement on the problem(s) to be solved, alternatives to identity systems should also be considered as potential solutions to whatever problem(s) is identified and agreed upon.
- The goals of a nationwide identity system must be clearly and publicly identified and deliberated upon, with input sought from all stakeholders; public review of these goals prior to selecting a proposed system is essential.
- Proponents of such a system should be required to present a very compelling case, addressing the issues raised in this report and soliciting input from a broad range of stakeholder communities.
- Serious consideration must be given to the idea that—given the broad range of uses, security needs, and privacy needs that might be contemplated—no single system may suffice to meet the needs of potential users of the system.
- Care must be taken to explore completely the potential ramifications, because the costs of abandoning, correcting, or redesigning a system after broad deployment might well be extremely high.

The legal, policy, and technological issues associated with nationwide identity systems warrant much more detailed and comprehensive examination and assessment than are presented in this report. The committee hopes that the extensive set of questions and issues raised here will help to both further and inform the policy debate. The committee welcomes feedback on this brief report as it continues preparing its broader and more in-depth final report on the topic of authentication technologies and their privacy implications.

http://www.nap.edu/openbook/0309084030/html/3.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

1 Introduction and Overview

While the events of September 11, 2001, have galvanized a search for improvements in the safety and security of our society, the challenge is to provide protection without sacrificing fundamental freedoms. An idea that has resurfaced as a result of the attacks is the creation of a "national identity card," often referred to simply as a "national ID."[1] This term is a bit of a misnomer, in that a card would likely be but one component of a large and complex nationwide identity system, the core of which could be a database of personal information on the U.S. population. This report by the Committee on Authentication Technologies and Their Privacy Implications provides a limited exploration of such a system and of the potential legal, policy, and technical challenges that it might present.

No one really knows if a nationwide identity system could detect or deter terrorism, although several arguments have been advanced. One is that such a system could be used to easily identify known terrorists upon their interaction with particular agents (such as airline security officials), and thus facilitate their arrest. On the other hand, unless the database of suspects includes a particular individual, the best possible identity system would not lead to apprehension. Another suggestion is that the data collected from the widespread use of nationwide IDs could help prevent terrorists from achieving their objectives. This might involve the detection of abnormal or suspicious patterns of behavior that accompany the planning and/or execution of a terrorist act.

Another potential role of a nationwide identity system is as an investigative tool in the aftermath of a crime or terrorist attack. Here, the data collected help retrospectively in the identification, arrest, and prosecution of the perpetrators. Some argue that this is primarily (though not exclusively) a post facto activity, more useful for law enforcement than for counterterrorism, which is in part a priori an *intelligence* function.

Terrorism issues per se are beyond the scope of this report, which examines the concept of a nationwide identity system in the large, not solely with respect to counterterrorism. The committee believes that the concept of a nationwide identity system—including *whether* such a system is a good idea—must be examined on its own merits.

Indeed, nationwide identity systems have been sought for many purposes in addition to countering terrorism. They have been proposed to aid in fraud prevention (for example, in the administration of public benefits), catch "deadbeat dads," enable electoral reforms, allow quick background checks for those buying guns or other monitored items, and prevent illegal aliens from working in the United States.

Depending on the nature of the population, the data collected, and the scope of use, a nationwide identity system could possibly help with other tasks as well. For example, a robust, accurate and comprehensive system might aid law-enforcement officials in tracking or finding people.[2] It is possible that the correlation of social (for example, health, economic, demographic) information could be more easily accomplished with the use of a national identity system; statisticians, for example, note how a single identifier would facilitate some of their analyses. In addition, depending on implementation choices, e-commerce and e-government transactions might be simplified. However, there could also be negative consequences, ranging from infringement on rights

[1] See, for example, "States Devising Plan for High-Tech National Identification System" at <http://www.washingtonpost.com/wp-dyn/articles/A32717-2001Nov2.html> and "National ID Card Gaining Support" at <http://www.washingtonpost.com/wp-dyn/articles/A52300-2001Dec16.html>.

[2] Examples include tracking fugitives, executing warrants, tracking noncitizens with expired visas, tracking illegal aliens, and confirming alibis for those innocent of criminal charges. A nationwide identity system could well facilitate the work done by the National Crime Information Center, a computerized database at the Federal Bureau of Investigation that permits access by authorized users to documented criminal justice information.

http://www.nap.edu/catalog/0309064303/html/4.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

and liberties (including loss of or invasion of personal privacy) to harm resulting from misidentification or misuse of the system, plus significant implementation and deployment costs. The trade-offs (enhanced security versus risks to privacy, cost versus functionality, and so on) need to be carefully considered.

Many other countries have nationwide identity systems, which they often use for such diverse purposes as proof of age (e.g., Belgium), proof of citizenship, and for generating electronic signatures (e.g., Finland). In the United States, citizens' concern for civil liberties, their historic association of ID cards with repressive regimes, and states' rights concerns have discouraged movement toward a governmentally sanctioned nationwide identity system.[3] Additionally, because the country was settled by immigrants, a significant fraction of whom wanted to escape just such practices, many U.S. record systems were intentionally designed not to gather linking data.[4] Further, it appears that laws requiring individuals to show proof of legal status or citizenship result in increased discrimination based on national origin and/or appearance.[5] The human rights issues that could arise, such as increased demands for documentation from those who look or sound "foreign" and the deterioration of living and working conditions for aliens, are substantial.[6] Clearly, an examination of the legal and social framework surrounding identity systems, while outside the scope of this report, would be essential.[7]

Although discriminatory acts such as those alluded to above could possibly be constrained by law, the presentation of identifying documents—driver's licenses and credit cards, for example—is being demanded today in more and more generic circumstances. There is also evidence of growing efforts in the public and private sectors to collect, maintain, correlate, and use more and more information on citizens' activities based on existing identifiers such as Social Security numbers (SSNs). Initially designed only for administering social security benefits, SSNs are now common data elements in public and private sector databases, allowing for easy sharing and correlation of disparate records. This is a classic example of "function creep"—continuous expansion in the use of a system first intended for a limited purpose.[8]

---

[3] The Electronic Privacy Information Center has compiled a set of resources and reports on the topic at its Website, <http://www.epic.org/privacy/id_cards/>.

[4] An example that frustrates many genealogists is that U.S. birth certificates, which usually require identifying the town of birth only of parents born in the United States; for people born elsewhere, the country of birth is sufficient. Generally speaking, the mindset that such things are "no one's business" has deep roots.

[5] See U.S. General Accounting Office, *Immigration Reform: Employer Sanctions and the Question of Discrimination*, March 1990; Marvin Howe, "Immigration Law Leads to Job Bias, New York Reports," *New York Times*, February 26, 1990, p. A1. The GAO report on IRCA (the Immigration Reform and Control Act of 1986) cites a "widespread pattern of discrimination" resulting "solely from the implementation of IRCA." Ten percent of employers discriminated on the basis of foreign accent or appearance, and nine percent discriminated by preferring certain authorized workers over others.

[6] Especially for communities of recent immigrants, there is likely to be significant controversy in shifting to a system that would prohibit or make difficult work and other activities without presentation of an ID. In considering the feasibility and desirability of a particular approach, designers of any such system should be aware of this potential opposition, as well as possible opposition from other segments of the population.

[7] It would be useful to examine how such systems have worked in other countries, as well as to examine nations where IDs have been proposed but not implemented (such as the United Kingdom).

[8] Some might argue that the Social Security number (SSN) is already a de facto national identifier. The General Accounting Office makes this assertion and also points out that no one law governs the use of SSNs. While originally intended to identify retirees who qualified for the Social Security retirement system, the SSN is now required, in some cases by law, to be used to identify individuals who seek federal assistance. In addition, of course, the SSN has been adopted as a taxpayer ID number. In his book *Database Nation*, Simson Garfinkel provides a history of the expanded use of the SSN. Provisions of the Social Security Act, the Privacy Act, and the Computer Matching Act are among the laws that attempt to limit under what conditions SSNs and

http://www.nap.edu/openbook/0309084303/html/5.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

Before any decisions can be made about *whether* to attempt to formalize some kind of nationwide identity system, the question of *what* is being discussed must be answered. Thus the committee believes that substantive and sustained analysis is needed on the issue.

There is no recognized universal model for a nationwide identity system. Because different people mean different things when they discuss the concept, evaluating it requires clarification of what is intended. The range of possibilities for identity systems is broad and includes alternative approaches such as the following:

- A database establishing a unique identity and maintaining information on every U.S. citizen, including, for example, information on known felony convictions and place of residence, available for government and commercial query;
- A system similar to the preceding systems that also includes noncitizens who are legally in the United States;[9]
- A database of only a fraction of the country's population—those individuals who have a specific characteristic (for example, criminal record, past noncriminal but anomalous behavior, trusted travelers, etc.)—that would not include the majority of people in the country; and
- A database allowing voluntary participation in return for such benefits as ease of entry into the country or access to the "fast line" at the airport security checkpoint.

The above possibilities (there are others as well) emphasize the need for answers to a number of questions before a more substantive analysis can proceed. Several policy questions should be asked when considering any kind of identity system (See also Figure 1.1):

- What would be the *purpose of the system*? Possibilities include expediting and/or tracking travel, prospectively monitoring citizens' activities in order to discern suspicious behavior and retrospectively aiding in the identification of perpetrators of crime, among others.[10]
- What is the *scope of the population* that would be issued an ID and, presumably, whose activities would be recorded in the system? How would the identities of these individuals be authenticated?
- What is the *scope of the data* that would be gathered about individuals participating in the system and correlated with their national identity? While it may be referred to casually as an "identification system," implying that all the system would do is identify individuals, many proposals talk about the ID as a key to a much larger collection of data. Would these data include only identity data (and what, precisely, is meant by identity data)? Or would other data be collected, stored, and/or analyzed as well? With what confidence would the accuracy and quality of this data be established and subsequently determined?

---

associated data are used (General Accounting Office, *Social Security: Government and Commercial Use of the Social Security Number Is Widespread*, GAO/HEHS-99-28, February, 1999). For example, the Privacy Act of 1974 <http://www.usdoj.gov/foia/privstat.htm> requires the disclosure of how the SSN will be used by all government agencies. In 1986, the Office of Technology Assessment addressed the issue of ubiquitous use of the SSN as well (U.S. Congress, Office of Technology Assessment, *Government Information Technology: Electronic Records Systems and Individual Privacy*, OTA-CIT-296, Washington, D.C., U.S. Government Printing Office, June 1986).

[9] Note that there are additional discussions about systems aimed exclusively at noncitizens, including, for example, proposals that would more rigorously track foreign students within the United States.

[10] In general, the narrower the goals, the simpler and, perhaps, less controversial a system is likely to be, although even a narrowly focused system can run into function creep and problems associated with mis-identification.

http://www.nap.edu/openbook/0309084309/html/6.html, copyright . 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

- *Who would be the user(s)* of the system (as opposed to who would participate in the system by having an ID)? One assumption seems to be that the public sector/ federal government would be the primary user, but what parts of the government, in what contexts, and with what constraints? In what setting(s) in the public sphere would such a system be used? Would state and local governments have access to the system? Would the private sector be allowed to use it? What entities within the government or private sector would be allowed to use the system? Who could contribute, view, and/or edit data in the system?
- What *types of use* would be allowed? Who would be able to ask for an ID, and under what circumstances? Assuming that there are datasets associated with an individual's identity, what types of queries would be permitted (e.g., "Is this person allowed to travel?" "Does this person have a criminal record?")? Beyond simple queries, would analysis and data mining of the collected information be permitted? If so, who would be allowed to do this kind of analysis and for what purpose(s)?
- Would participation in and/or identification by the system be *voluntary or mandatory*? In addition, must participants be aware of or consent to having their IDs checked (as opposed to, for example, allowing surreptitious facial recognition)?
- What *legal structures* would protect the system's integrity as well as the data subject's privacy and due process rights, and define the government and relying parties' liability for system misuse or failure?

These questions will drive technological considerations (described in Section 3), including what kinds and what levels of system security would be required.

Throughout this document, the term "nationwide identity system" is used in lieu of the more colloquial "national ID" or "national ID card." Many of the proposals are often presented in terms of a national identity *card*, though technologies exist—possibly including biometrics, which measures and analyzes unique physiological and behavioral characteristics of individuals—that might serve some of the same proposed purposes without requiring a physical card. Nevertheless, the emphasis in this report is on card-based models simply because they have been proposed most frequently. In addition, many of the policy questions and database-related technical issues apply both to card-based systems and those that do not require a physical card (see Chapter 3).

With respect to the chosen phrase nationwide identity system, "nationwide" is meant to underscore the scale (both geographic and in terms of numbers of users) needed, without the implication that IDs would be necessarily be generated from a single central location or, implicit in the term "national," that only citizens would need an ID.

The notion of identity is complicated, even when discussing only identity of persons (and not things, arguments, systems, etc) as this report is doing. This report distinguishes between an identifier (the name or sign by which a person is known), which can be thought of as a label by which an individual is known in and to society and with which he or she conducts his or her affairs within society, and the identity of a person as seen by others. Specifically, for purposes here, the term "identity" refers to a set of information about a person X believed to be true by Y. More colloquially, identity is associated with an individual as a convenient way to characterize an individual to others. The set of information in combination with the identifier (name, label or sign) by which a person is known is sometimes referred to as that person's "identity," as well. The choice of information may be arbitrary, linked to the purpose of the identity verification (also referred to as authentication) in any given context, or linked intrinsically to the person—as in the case of biometrics (see Box 1.1).[11]

[11] Although biometrics are proposed with increasing frequency for a variety of identification and authentication purposes, they pose many difficult issues for system design, implementation, and use. These will be explored in the committee's final report.

http://www.nap.edu/openbook/0309084350/html/7.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

For example, the information corresponding to an identity may contain facts (such as eye color, age, address), capabilities (for example, licensed to drive a car), medical history, financial activity, etc. Generally, not all such information will be in the same identity, allowing a multiplicity of identities, each of which will contain information relevant to the purpose at hand. The term "identity" is used in the phrase "nationwide identity system" to emphasize that decisions must be made about what constitutes an identity within a system and *that* an identity would be established for participants.

A critical question—which goes beyond the scope of this report, but which must be considered in the larger law-enforcement and national-security context—is whether establishing and verifying identity is either necessary or sufficient for achieving any of the desired objectives of the system. It may be that they require collection and analysis of data, and/or prospective or retrospective tracking or surveillance, well beyond mere identity verification.[12] Note that even the question of whether to institute collection of data and surveillance is not binary (See Box 1.2).

"System" may be the most important (and heretofore least discussed) aspect of the term nationwide identity system because it implies the linking together of many social, legal, and technological components in complex and interdependent ways. The success or failure of such a system is dependent not just on the individual components, but on the ways they work—or do not work—together. Each individual component could, in isolation, function flawlessly, whereas the total system failed to meet its objectives.[13] The control of these interdependencies, and the mitigation of security vulnerabilities and their unintended consequences, would determine the effectiveness of the system.

A nationwide identity system would also consist of more than simply a database, communications networks, card readers, and hundreds of millions of physical ID cards. The system would need to encompass policies and procedures, and to take into account security and privacy considerations and issues of scalability, along with human factors and manageability considerations (if the requirements of use prove too onerous or put up too many barriers to meeting the goal of the relying party, he or she may well try to bypass the system). The system might need to encompass the participants who will be enrolled, the users (individuals, organizations, governments) who would have access to the data, the permitted uses of the data, and the legal and operational policies and procedures within which the system would operate. In addition, process would need to be in place to register individuals, manipulate (enter, store, update, search and return) identity information about individuals, issue credentials (if needed), and verify search requests, among other things. The term "system" is used to emphasize the complicated nature of what would be required in a way that the colloquial phrase "national ID card" does not.

It is important to note that a variety of identity systems fit within the scope of what is being

[12] For example, if the goal were to track the activities or whereabouts of an individual to detect illegal activity or suspicious patterns, surveillance of the behavior and activities of said individual would be needed after identification was accomplished. Surveillance might require a warrant or other judicial intervention, depending on the approach taken. If the goal were to detect suspicious activity by previously unsuspected individuals (in order to prevent illegal activity), *correlation* of surveyed actions would be required after identification and surveillance were accomplished. Such correlation would presumably have to be done before establishment of probable cause for a search in order for it to be useful.

[13] There are examples of this in security mechanisms—for example, where individual techniques to provide additional security interact unexpectedly in such a way as to make the system less secure. Charles Perrow explores the broad concept more thoroughly in *Normal Accidents*, McGraw-Hill, 1986. In addition, the Web site <http://www.safeware-eng.com/software-safety/accidents.shtml> describes the distinction between component failure accidents and system accidents.

http://www.nap.edu/openbook/0309084030/html/8.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

discussed in this report. The recent AAMVA[14] proposal to link state motor-vehicle databases is a nationwide identity system. So is the recent proposal to create a traveler ID and database to expedite security checks at airports. Each of these systems could and should be subjected to the kind of analysis and critique described in this report. Some of the issues raised here will be more applicable to some systems than to others, but virtually any large-scale identity system will need to take into consideration a number of policy and technological issues; in fact, before deciding to build any identity system, the issues outlined in this report should be explored.

A top-down, monolithic system controlled by the federal government is not the only kind of nationwide identity system that this report addresses. For example, unifying document formats and linking state driver license and ID issuing system databases would provide broad (though not complete) coverage without creating a federally controlled national ID system. Further, an examination of the successes and failures of the variety of nationwide identity systems in use in other countries would be necessary in order to have a fully informed discussion within the United States. However, when studying such systems, questions of scale must be kept in mind. Experience with a system for a population of tens of millions is not necessarily applicable to a system that might incorporate hundreds of millions. In any case, many of the questions raised in this report assume large-scale systems and widespread participation in and use of such systems.

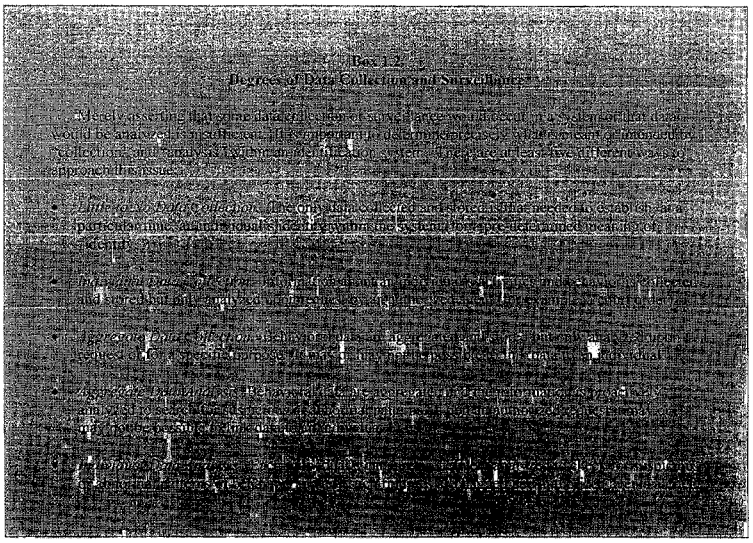
Without attempting to answer comprehensively the many questions surrounding a nationwide identity system and without making assertions about whether to move toward or away from a nationwide identity system, the report aims to highlight some of the significant policy, procedural, and technical challenges presented by such a system, with the overall goal of prompting a broad discussion among and between policy makers and stakeholders.

This brief document is intended to inform the policy debate. Complete policy analysis is outside its scope, though several of the broad themes outlined here will be addressed more fully in the committee's final report. Chapter 2 describes what the committee believes is the most important issue in the debate—namely, the system goals—along with other policy issues that the committee believes should be considered in advance of implementation and deployment. Chapter 3 explores some of the technological issues involved in implementing a reliable and secure nationwide identity system while minimizing unintended consequences, such as compromises of privacy or the (possibility of) creation of new vulnerabilities. Chapter 4 offers concluding remarks and suggestions.

[14] See <http://www.aamva.org/> for more information. The committee received a briefing describing some of the issues facing AAMVA in developing a more secure driver's license infrastructure in a context where use of driver's licenses is expanding beyond their nominal function.

http://www.nap.edu/openbook/0309084300/html/10.html, copyright 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION



Box 1.2
Degrees of Data Collection and Surveillance

http://www.nap.edu/openbook/0309084309/html/13.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

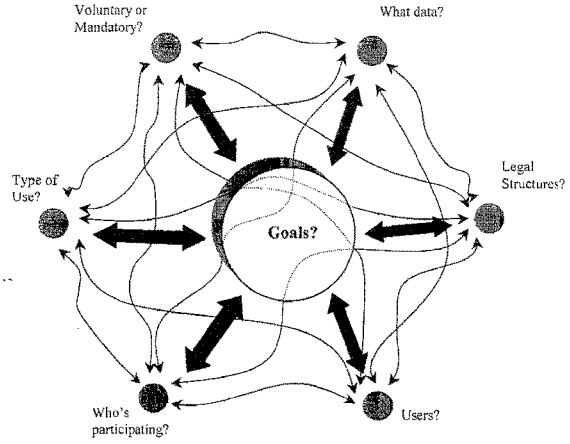


FIGURE 1.1 Interconnecting policy choices

The choices made for each of the questions posed will bear, with differing degrees of influence, on the choices made with respect to all of the other issues. For example, the goals of the system will influence what data are collected about individuals. What data are collected about individuals will constrain the possible goals of the system. Who is allowed to use the system will have a bearing on what legal structures are needed. What legal structures are put in place will bear on what kinds of access to the system are allowed. And so on.

http://www.nap.edu/openbook/0309043018/html/13.html, copyright 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

2 Policy Considerations

Numerous policy questions surround any proposed nationwide identity system. They require sustained deliberation by policy makers and significant input from the various stakeholders—including federal, state, and local governments and agencies, privacy advocates, public-interest groups, civil rights and liberties groups, and those who would participate in and use the system (that is, ID holders, ID requestors, and data analysts). Establishing a nationwide identity system would almost certainly be a complex and expensive process, requiring years of legislative, technical, and public relations work, as systems now in place elsewhere have shown.[1]

WHAT DOES IDENTITY PROVIDE?

Whether and when knowledge of "identity" could aid in solving a problem or meeting an objective depends in part on the word's very definition. For the purposes of this report, identity indicates sets of information (say, a database record or strongly linked system of records) about a person that can be used to tell who that person is. Confirmation (at some level of assurance) of identity is useful in contexts when one or more of the following are needed: (1) knowledge (in the present) about a person's past is sought (e.g., the use of a dossier), (2) knowledge about a person in the present needs to be remembered for use in the future (e.g., the creation of a dossier), (3) distinguishing between two individuals is required to prevent the possibility of mistaking one of them for the other, or (4) verification of identity information provided by a third party. Identification and/or authentication are generally used to aid in recognition when there are multiple dealings with a single individual but could also be relevant to a single experience/transaction. (Note that authentication presumes a proffered identity that needs to be confirmed, whereas identification does not—see Box 1.1.)

While colloquial discussions of IDs or ID cards may assume simple, unique pairings of information and individuals, reality is often more complicated. In practice, individuals often have multiple identities—to family, to an employer or school, to neighbors, to friends, to business associates, and so on. Thus, different sets of information are associated with an individual in different contexts—and sometimes an ID card or equivalent is relied upon to provide or point to that information. For identity systems that have existed in our society for some time, there is a common understanding of what information is associated with each. A record associated with a driver's license, for example, includes traffic violations; a record associated with a credit card includes late payment information; and so on.

Multiple identities (that is, multiple sets of information corresponding to a single individual) may allow individuals to control who has access to what kinds of information about them, and the use of multiple identities can be a legitimate strategy for controlling personal privacy in an information society. In addition to a measure of privacy protection, the use of multiple identities, even with respect to a single organization, serves legitimate and desirable functions in societal institutions as well. One individual may have several distinct roles with respect to a particular organization. For example, as far as the IRS is concerned, one might be an individual taxpayer, an IRS employee, or the comptroller of a nonprofit organization.

If, however, colluding agents are willing to make the effort, they might be able to link an individual's records—through additional information or correlation with each other's information—to

[1] In the Philippines, for example, the Social Security System ID card project has been under active development and deployment for 6 years and has only reached an enrollment of just over 2 million, en route to the goal of enrolling 40 million social security beneficiaries, members, and dependents.

http://www.nap.edu/openbook/0309088308/html/14.html, copyright 2006 The National Academy of Sciences, all rights reserved

create a single record. In many cases, an identity will include a common cross-reference, such as a Social Security number, that makes it trivially easy to link it to other identities. Moreover, there are usually other possible cross-references (such as address, age, and so on) that enable different sets of information to be linked, though there may be institutional practices or practical barriers that discourage such linking.[2] In addition, questions arise as to how reliable the linking would be—some institutions may not mind if linkages are not completely supported, whereas others demand high levels of accuracy.

Sometimes, the use of multiple identities by a single person, or the use of a single identity by multiple persons, may be evidence of (or exploitable for) fraudulent behavior. Several criminals could use a single identity not considered problematic within the system, or a single terrorist could use the least suspicious of multiple identities accessible to him for boarding a plane. In principle, a nationwide identity system could, in some contexts, eliminate or significantly reduce these sorts of problems if it is designed to prevent both multiple individuals from claiming a single identity and multiple identities from being claimed by a single person.[3]

One implication of the term national ID is that these identities are centrally managed in order to make it difficult, if not impossible, for one person to have multiple identities. A system designed to link a person to a single identity (and prohibit use of multiple identities by a single person) within a certain domain must be mandatory (that is, everyone within the domain of interest must be included in the system), otherwise those wishing to establish multiple identities would simply opt out of the program. Also, checking is essential at the time an individual joins, to be sure that he or she is not already in the system. If an identity reveals potentially damaging information about a person, the person may try to avoid the entry of this information into the system by creating a different identity. In some cases, this capability is controlled by having only one central registry for the identity information.[4]

Depending on the goals of the system, creating a tight identity-to-individual bond might be excessive. Often it doesn't matter exactly who someone is as long it is clear that he or she is a member of a particular group (e.g., over 21 or an officer of a corporation with check-signing privileges). Such group identities are often extremely useful in expediting matters in certain contexts and may raise fewer privacy concerns.

Thus, any proposal for a new identity system requires a discussion of what sorts of identity information would actually be relevant and helpful to the stated goals of the system.[5] It also requires

---

[2] See the1997 CSTB report *For the Record: Protecting Electronic Health Information.*

[3] Historically, the Social Security Administration (SSA) allowed husbands and wives to share a single Social Security number and some grandfathered couples still do. Thus, such an SSA "identity" refers to two people. Similarly, children and one of their parents can share a single passport and passport number. More commonly, the case of two or more individuals maintaining a joint bank account illustrates one identity (the bank account and associated information) being shared by multiple individuals. Creating multiple identities out of the single record set would be extremely hard for the issuing agencies, because the linked people usually share a single last name. Splitting the record, therefore, might require additional personal information.

[4] A current example of a system that attempts to disallow multiple identities is the Commercial Driver's License Information System (CDLIS). U.S. federal law—the Commercial Motor Vehicle Safety Act of 1986 (PL 99-570)—prohibits commercial truck drivers from having multiple driving identities. In compliance with the law, CDLIS is used by the states—via a centralized system that links the various issuing (state) agencies—to check that multiple licenses are not issued. However, nothing in the CDLIS system itself prevents multiple drivers from using this single license and, in fact, fraud of this type has been documented (see "Biometric Identification Standards Research: Final Report Volume I," San Jose State University, December, 1997, <http://www.engr.sjsu.edu/biometrics/fhwabiom.zip>).

[5] If the goal of the system is to aid in counterterrorism, then relevant questions might include the following: Is a past criminal record a signal of a potential terrorist? Is a long record of frequent travel a signal that a person is or is not likely to be a terrorist? And so on.

http://www.nap.edu/openbook/0309084393/html/15.html, copyright . 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

taking into account the levels of confidence with which information was associated to an individual, since basing a system on fragile or unreliable data poses numerous risks. In addition, in some cases there are legal restrictions on what sort of information may be asked of an individual (presumably to include in that person's associated identity information)—for example, it may not be legal to take into account a person's race, gender, national origin, religion, and so forth. In other cases, retaining the advantages that come with the ability of an individual to maintain multiple identities or to maintain group identities could also be desirable. All in all, establishing what is meant by "identity" in a nationwide identity system—in other words, which collection of information is meant to encapsulate an individual's distinctiveness—is a first-order concern.

TO WHOM AND FOR WHAT?

Once the notion of identity has been articulated, a determination must be made as to who would be issued an ID (see box 1.1 for the distinction between "ID" and "identity") and for what purpose. First and foremost, the goals and requirements of the system must be carefully articulated. What problems should the system be designed to solve? How would it provide solutions to those problems? Without a priori decisions about what types of system functions, determined by policy choices, are desired, the software and hardware may impose unwanted or undesirable restrictions or allowances.[6]

If a goal of the system is the identification and/or tracking of non-U.S. nationals, then issuing IDs only to U.S. citizens would not be sufficient. Identification and tracking of all individuals would be required.[7] Furthermore, non-U.S. nationals are already required to have IDs when in the United States (passports and, in some cases, visas); however, there is likely to be less control over—and therefore less confidence in—such foreign-issued credentials. This raises questions about international coordination, cooperation, and harmonization.[8,9] The problems now present in keeping track of passports and visas, and in assuring that the right individuals and agencies have the

[6] See Lawrence Lessig's treatment of software imposing values in *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.

[7] The terrorist attacks of September 11, 2001, were carried out exclusively by non-U.S. nationals; none of them would have had a U.S. ID if one were required only of citizens. In addition, undercover operatives sponsored by a major foreign group or state hostile to the U.S. generally are individuals without suspicious records. It follows that such people's IDs (be they within a U.S. nationwide identity system or outside) would not contain anything particularly problematic.

[8] The logistical considerations involved in issuing high-security identities for everyone entering the country are significant, especially when individuals do not need visas in advance (such as citizens of countries in the Visa Waiver Program).

[9] Even if IDs were issued to foreign visitors entering the U.S., the information would be based on information provided by their country of origin. Its usefulness is limited for at least two reasons: (1) many countries do not have much data about their citizens to begin with, and others may be unlikely to provide other nations with suspicious background information about their own citizens and (2) even if a country indicates that an individual seeking admission to the United States has a problematic background record, that doesn't mean the United States would consider such a person a risk (for example, a country might provide warnings about political dissidents). Adding information to an individual's ID beyond what their country of origin provides (presumably gathered by U.S. Intelligence) is problematic for a number of reasons, including cost, scale, paucity of data, and potential compromise of sources and methods behind the information.

http://www.nap.edu/openbook/0309084030/html/16.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

appropriate data when needed, would undoubtedly persist in a new identification system.[10] They also serve to demonstrate how difficult it is to implement a large identification system that is also robust.

What Is Required for ID Issuance?

The best that any system of authentication can do is provide a compelling connection with some previous verification of identity. Accordingly, trust in the integrity of the system is based not so much on the first such verification as on increasing confidence when all previous transactions with that particular individual have worked out.[11] But at the outset, upon determination of who should have IDs, a host of questions arise: How is identity first established within the system? What information would be required of an individual upon application? How would that information be verified?

Such broad questions imply others that are more specific: How would the "true" identity of individuals be established (e.g., for individuals in the initial stages of a program or after card loss or destruction)? What family name(s) would be used for the individual (birth name, adopted name, married name, father's name, father's mother's name)? Could middle names, diminutives, or nicknames be used as first names? When can or must these names be changed? How would people with similar or identical names (or other pieces of associated data) be differentiated in the system? If participation in the system were mandatory, at what point in a person's life would the ID begin to be required? How frequently would renewal be required? Under what circumstances would reissuance be required? What if the system "loses" a person (that is, a person claims to be in the system, but his or her information is not accessible)?

What Is the Meaning of an ID?

Broader, and perhaps more important, is the meaning of the ID (that is, the identity information about a person in the identity system and its associated token). Would the law define rights, privileges, and obligations with respect to the ID? Would the law define a legal person in terms of the ID, or vice versa, or neither? Related to the meaning is the issue of a citizen's and the government's responsibilities with respect to a nationwide identity system. A host of legal issues arises if an ID is to have significance as, say, a government-authorized identification token. Using an ID to verify a person's identity would not be of value without an obligation to present it upon demand by authorities or in an authorized search of one's person.[12]

Questions that would need to be addressed include the following: When must the ID be carried? When must it be presented to a government official? What happens if the holder refuses to present it? What happens if the ID has been lost or stolen? How can information on the ID (or associated with it) be changed, and by whom? What if the infrastructure is down and the ID cannot be verified? Can only the federal government compel the presentation of the ID, or would state and local government officials (which is where most law-enforcement occurs and many social services are delivered) also have such authority?[13]

---

[10] As an example of this, the *Washington Post* reported that 15 of the September 11 hijackers applied for visas in Saudi Arabia, where officials have indicated that identity theft is a serious concern. See <http://www.washingtonpost.com/wp-dyn/articles/A14788-2001Oct30.html>.

[11] Although trust developed in this fashion is vulnerable as well. For example, individuals may act in a completely trustworthy fashion for a long period of time and then behave fraudulently or criminally.

[12] Other identification techniques, such as facial recognition, might not require an obligation to present an ID.

[13] For example, if the goal were to locate and keep track of non-U.S. citizens and/or known criminals within the United States, it would likely be necessary to challenge all individuals (including citizens) to present

http://www.nap.edu/openbook/0309086396/html/17.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

Where Does the Identity Information Reside?

These questions point to other questions that must be considered about the information associated with a person's ID. If it is a card or other physical token, what information is stored on it in human-readable format on the ID? What information does the ID store in machine-readable format? What information about or pertaining to an individual is stored in the identity system's databases? What information in those databases is explicitly linked to information in other databases? Who has the authority to create these linkages? Who can access which information about a person in the system? What algorithms are used to analyze data in order to make assessments about a particular individual in a particular context (e.g., risk profiling)?[14] (See Figure 2.1 for a description of what can happen to identity information within a system.)

Many of the questions raised in this section point more broadly to the problem of controlling function "creep" (as mentioned in Chapter 1). Decisions and policies made for one kind of system may not apply well if that system begins to be used for other than its original purposes. In the context of an identity system, function creep can occur when the same ID/token is used to access multiple systems. (This has happened with driver's licenses in that they are used not only to prove authorization to drive, but also for proof of age and proof of address in various contexts.) Reuse of an ID/token for purposes beyond the original intent leads to the feasibility of correlating information from many different sources and systems, which can be a cause of concern in many instances, particularly with respect to privacy. Strategies and policies that prevent or constrain function creep will be an important factor in any identity system.

PERMITTED USERS OF THE SYSTEM

Another set of policy questions arises over users of a nationwide identity system (recall that a system encompasses numerous social, legal, and technological aspects): May only the government use or request an ID? Under what circumstances? Which branches (federal, state, local) of the government? May any private person or commercial entity request presentation of an ID within the system? May any private person or commercial entity require presentation of an ID? Would certain private-sector organizations be required to use, ask for, and verify IDs? If so, there is a possibility that such mandates might be interpreted as a safe harbor with respect to some liability questions. How would that be handled? Who may use the information on (or associated with) the ID, and for what? Who may enter or modify information associated with the ID?

Depending on the goals of the system, use of the system by the private sector may be necessary. For example, if the goal is to create a database to mine for suspicious activities, tracking of a broad class of activities in the private sector may be viewed as critical. Thus, in order to accomplish this tracking, the ID would need to be presented in connection with many transactions in

---

the card at regular intervals and/or for a wide variety of activities. It would further be necessary to require all individuals to carry the card at all times. It could be that many forms of purchases and transactions would require use of the card in an ancillary fashion, in the same way that purchases with a check often require the presentation of a driver's license or equivalent form of photo identification. In this way, the information associated with the card (and by extension with the holder's identity) would become part of the records generated by some set of interactions, just as Social Security numbers and license numbers are used today—a practice that suggests the development, in effect, of dossiers. A question then arises as to what an individual's failure or refusal to present the card under these circumstances would mean.

[14] The European Data Protection Directive mandates a limited right of individuals to know what algorithms are used to make decisions about them on the basis of personal information.

http://www.nap.edu/openbook/0309084385/html/18.html, copyright . 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

the private sector (e.g., when traveling on commercial airlines, when purchasing weapons, or when staying in a hotel.) However, as the set of users of a system expands, securing against misuse becomes more complicated. Widespread use (and abuse) of the information associated with an ID is a major concern, emphasizing the ultimate effect of initial policy choices about the goals and purpose of the system.

Management and Operations

Determining how any nationwide identity system should be managed and operated will be a key issue. If the federal government were to play a leading role in operations and management, an overhaul of business and management practices at multiple levels may be necessary.[15] In addition, worldwide coordination would likely be necessary. For example, depending on the system goals, ID issuance by U.S. consulates abroad may have to be allowed, raising the potential for fraudulently issued IDs. Pragmatically, even the most secure documents issued by the U.S. government (passports, green cards, and even currency) have been forged with regularity. Requiring federal government management and operations expertise for nationwide identity systems thus raises a host of issues that must be taken into consideration.

Another set of policy issues involves the roles of the public, private, and not-for-profit sectors in a nationwide identity system. For example, in place of the above scenario (in which the federal government takes responsibility for the management and administration of a nationwide identity system), the private sector alone might develop and maintain the system. Alternatively, the private sector could be subordinate to some procuring federal agency, in which case any resulting data would be subject to federal laws such as the Privacy Act, the Computer Matching Act, the Government Information Security Reform Act, and the Computer Security Act.[16]

Of course, some hybrid model—featuring a public/private partnership—is also possible, though it would require explicit designation of which sector is responsible for what and who might be liable to potentially aggrieved parties when errors or abuses occur. (In particular, careful attention should be paid to due process issues that may arise in connection with error correction.) In any case, it would be absolutely necessary to define how a single organization's private role in enabling the system should relate, if at all, to that same organization's private role in its use. Furthermore, how the private entity would be funded would also be an issue. Moreover, the goals of private institutions with respect to such a system are likely to be very different from those of public institutions.[17] This

[15] Since passage of the Paperwork Reduction Act of 1995, the Office of Management and Budget has been challenged to manage complex information assurance issues, even though it has both budgetary and statutory authority. The Department of Defense, as another example, is charged with managing classified and other national security systems. Nationwide identity systems pose new problems for each of these organizations. If the federal government were to attempt oversight of the system, it would be necessary to determine an appropriate management model suited to undertaking management of large-scale identity systems.

[16] The acts all impose regulatory requirements on federal agencies that collect, use, and maintain sensitive information. The Privacy Act and the Government Information Security Reform Act in particular impose significant public notice and comment requirements on federal agencies to ensure public participation in the appropriateness of planned agency uses of data. The Computer Security Act imposes a risk-based standard for agencies to ensure they protect the confidentiality, integrity, and availability of sensitive federal information and supporting systems. If a nationwide identity system turned out not to be a federal government system, these laws would not apply and the protections they offer would not be available to individuals whose information is housed in the system.

[17] For example, a small store owner probably is not as interested in customers' individual identities at point-of-sale transactions as he or she is in receiving assurance that payment will be made.

http://www.nap.edu/openbook/0309084830X/html/19.html, copyright , 2001 The National Academy of Sciences. all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

difference in ultimate objectives could lead to significantly different system requirements and design and could encourage function creep over time.

PERMITTED USES OF THE SYSTEM

A key question about a nationwide identity system is the uses to which the information in it will be put. Will the system be designed to foster consolidation of other (especially federal) databases—or might that be a predictable side effect? Will it be designed to support individualized queries about individuals or provide a yes/no answer to simple questions (for example, Is this individual a U.S. citizen?)? Will the system facilitate data mining to establish "suspicious profiles?" If the system is to be used extensively by law enforcement, checks and balances would need to be put in place to prevent misuse of information (for example, constraints should be placed on how information collected or seen—perhaps tangentially—as a result of a particular investigation can be used for other purposes).

Consider the system's potential need to make real-time associations of persons with identity—a policy question with technology-challenging implications. For many purposes, the linkage between the person and the identity need not be provided instantly. An application for a mortgage need not be processed in seconds. On the other hand, an identity that authorizes access to a secure building must be validated at the time of the intended entry. A related issue is the prospect of constant real-time correlation and analysis of an individual's national-identity-based transactions.[18] It is likely that such correlation, while possibly desirable depending on the goals of the system, would be financially, technologically, and administratively impossible. For that matter, even retrospective correlation of all transactions would be extremely challenging and expensive. Depending on what information must be tracked and stored, very large amounts of data may be generated. And the analysis of large amounts of data while looking for certain kinds of patterns is a large and open research area.

An additional correlation concern relates to potential uses beyond those associated with public safety and counter-terrorism. If private entities are allowed to use the nationwide identity system for their own purposes, it is likely that IDs would be linked to a wide range of information, including bank accounts, credit cards, airline tickets, car rentals, hotel stays, retail transactions, purchases of controlled items (guns, explosives, perhaps some fertilizers, prescription drugs subject to abuse), phone lines, cell phone accounts, prepaid cell phones, and so on.[19] Even if the data were not explicitly tied together by organizations, linking users by data items in their identity (such as SSNs) is possible. In addition, systems that employ biometrics could have the ability to link individuals whose information was stored in different databases. That is, two different digital representations of an iris or fingerprint could be compared to see if they might have come from the same eye or finger.[20,21]

[18] For example, it may be useful to correlate instantly the renting of a large truck in one state with the purchasing of a large amount of fertilizer a day later in another state.

[19] The issues become even thornier when one considers the possibility that physical items may eventually have their own tracking systems embedded in them. Cross-correlation of information about things *and* people would likely result in an exponential explosion of data, further complicating the technical questions and confounding the privacy issues. See Charlie Schmidt's "Beyond the Bar Code," *Technology Review*, March 2001.

[20] Systems that will allow eye/finger versus database comparisons but not database versus database comparisons have been proposed, such as in N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing Security and Privacy in Biometrics-Based Authentication Systems," *IBM Systems Journal*, vol. 40, No. 3, 2001. Another possible solution would be to use biometrics only at three points in any given system: when checking for duplicate enrollments at initial registration to prevent issuance of multiple IDs to a single user, when

http://www.nap.edu/openbook/0309084098/html/20.html, copyright, 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

Finally, privacy is of serious concern to many, especially when information linkages extend across the boundaries of multiple identities—for example, in the linking of health data, credit ratings, or organizational memberships with our employment records. Of greatest concern to most people is the creation without authorization of such linkages by others, particularly those in positions of authority—governments or employers, for example.

The "minimization principle" is often used as a guideline when building systems sensitive to privacy concerns.[22] It relates to the kind and quantity of information collected from and/or about individuals and emphasizes the need to collect only the minimum amount necessary for the desired transaction. Minimization also implies that disclosure of information should be limited to the purpose(s) for which it was collected. A pragmatic reason for this, in addition to the privacy aspects, is that information is likely to have an accuracy commensurate with its original purpose (for example, the address given on a video-store membership application form is more likely to be false than the home telephone number given on an employment application). In addition, the minimization principle suggests that information should be deleted when no longer needed and that the information disclosed be limited to that which is needed to fulfill the request (as opposed to disclosing all available information about an individual or transaction).

Clearly, minimization runs counter to the kinds of information collection and correlation needed for the preemptive and retrospective analyses contemplated by proposals for a nationwide identity system meant to counter terrorism and unlawful activities. Resolving or mitigating this tension will be a serious challenge to those developing policies for a nationwide identity system.

VOLUNTARY OR MANDATORY?

Whether participation in the system is to be required or chosen is a major policy decision. Until the goals of the system are clearly articulated, it is difficult to gauge which type of participation would be preferable. Some goals may directly or indirectly require mandatory checking of identities and/or enrollment in the system. For example, if the goal were to prohibit travel by persons with malicious intentions, all air travelers would need to be enrolled—if enrollment were voluntary, such people would simply not enroll and would be permitted to travel. In general, any attempt to ascertain that an individual does not possess an unwanted attribute (for example, a malicious intent) requires a complete knowledge of behaviors related to that attribute, and hence mandatory checks.

Clearly, a voluntary system is likely to meet with less resistance and to raise fewer concerns about civil liberties, although its voluntary nature would seem to limit the kinds of goals that it could expect to achieve. However, even when a system is nominally voluntary, attention should be paid to whether the large inconveniences of nonparticipation make it effectively mandatory. Deliberate consideration of whether and when to require participation and what the implications of widespread but voluntary participation would be are essential.

---

checking the binding between the card holder and the card at point-of-service applications, and when reissuing the card. This check, which could occur without revealing the biometric pattern to the holder of the card, would create yet another point in the system where security is needed.

[21] Work done by Latanya Sweeney (see <http://sweeney.heinz.cmu.edu/confidentiality.html>) suggests that very little information is needed to uniquely identity a particular individual in even an ostensibly anonymized database, suggesting that creating linkages between databases—even without biometric data tying individuals to their data—may not be difficult.

[22] This notion is articulated in a report of the U.S. Privacy Protection Study Commission, *Personal Privacy in an Information Society*, Government Printing Office, Washington D.C., 1977, also known as the Privacy Commission Report. Three principles espoused in that report are to (1) minimize intrusiveness, (2) maximize fairness, and (3) create legitimate, enforceable expectations of confidentiality.

http://www.nap.edu/openbook/0309084300/html/21.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

There are at least two levels at which participation occurs: when an individual establishes an identity within the system and when his or her ID is requested or used in a given interaction. Whether an individual must consent to presenting his or her ID as opposed to having the ID observed from a distance (possibly without the person's knowledge) is another critical policy decision.

WHAT LEGAL STRUCTURES?

In considering whether to implement any nationwide identity system, decision makers would have to determine whether and how such a system would be regulated, and by whom. What constitutes misuse of the ID or the data associated with it? What penalties are imposed on the holder for misusing or tampering with the ID? What penalties are imposed on officers of the government for abuse of the card or misuse of its information? What penalties are imposed on private parties or businesses other than the holder for abuse of the card or misuse of the identity and associated information? Would laws permit, discourage, or forbid private-sector actors from asking individuals to present the card for reasons other than those intended by the public sector?

Depending on the policy choices and deployment strategies a nationwide identity system reflects, its constitutional implications may be significant. The constitutional limitations on an agent's ability to require presentation of IDs[23], along with the limitations on the ability of Congress to enact a nationwide identity system, should be explored before any such enactment to avert the costs of imposing the system and then having to revise or abandon it in the face of its unconstitutionality, to say nothing of its effects on civil liberties.

Depending on implementation details and policy decisions, a nationwide identity system could be used to compile and store large amounts of information on individuals; the legal restrictions on compiling and using dossiers would have to be strictly obeyed. More broadly, an understanding of the principles that support significant privacy-related authorities, as well as the major legal traditions and principles that drive U.S. privacy law and policy, will be necessary when considering identity systems that will handle personally identifiable information.[24] In particular, it would be helpful to have insight into the statutory models that pertain where mistakes can have severe repercussions (such as census information collection or tax returns).

A further consideration is that because identification in the form of birth certificates and driver's licenses has traditionally been done at the state and local level, issues of states' rights and associated issues could well arise. It will be important to examine the federal/state constitutional tensions along with how such issues may facilitate or impede development of policy solutions in this arena. How, for example, should a nationwide identity system interact with the other federal, state, and local identity systems that are already in place? Should these other systems continue, be coupled to the nationwide system, or be superseded?

BENEFITS AND DRAWBACKS

Creation of a well-thought-out and well-designed nationwide identity system could have some advantages over the current methods of establishing and verifying identity, such as state-issued

[23] In fact, the Supreme Court has limited the situations in which government authorities and police officers may require individuals to leave an area due to lack of apparent purpose. See *Chicago v. Morales* at <http://supct.law.cornell.edu/supct/html/97-1121.ZS.html>.

[24] U.S. Department of Health, Education and Welfare, Secretaries Advisory Committee on Automated Personal Data Systems—Records, Computers, and the Rights of Citizens. Government Printing Office, Washington, DC, 1973.

http://www.nap.edu/openbook/0309084059/html/22.html, copyright . 2003 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

driver's licenses, Immigration and Naturalization Service documents, and birth certificates. Current systems have many characteristics that pose a challenge to meeting the goals expressed by proponents of a more uniform nationwide identity system. For example, the documents in current systems are not standardized in form or information content, so that a person inspecting an offered document often cannot determine if it even *resembles* an authentic document (much less whether it actually *is* authentic) without substantial research.

Similarly, such documents are generally not strongly linked to the person who offers one for identity, allowing several people to use a single authentic document. Identities also cannot be clearly revoked in current systems, allowing a person to successfully offer an invalid ID as verification of identity. Moreover, these systems do not universally employ strong anticounterfeiting measures, and existing countermeasures vary from document to document and are not easily checked.

A nationwide identity system, depending on its implementation, might drive many other forms of identification out of use by subsuming their functionality. Several factors in particular could encourage widespread third-party reliance on the nationwide identity system to the exclusion of current systems. First, if the cost of the system is borne by the government and its associated agencies, the system's use would be free to other segments of society, unless measures (technical, legal, or otherwise) are taken to prevent unauthorized use. Second, unless private parties are prevented by law (or restrictions on technology) from relying on the nationwide identity system, the liability associated with such reliance would be shielded by the government's sovereign immunity. Third, even if the private parties were forbidden to rely on the data, it is very likely that private commercial organizations would begin to correlate data about citizens based on their card and/or identity within the system. The information in these commercial databases may not be as strongly protected (legally or technologically) as, presumably, is the information in the nationwide identity system's own databases. The correlation and aggregation of personal information thus raise a variety of policy questions about the use of such information and constraints on it.

As Garrett Hardin wrote in 1968, "You can't do just one thing."[25] The introduction of a nationwide identity system would create ripples throughout society and the legal system. It is difficult to predict what unintended effects these ripples would have. In part due to our frontier history, there seems to be a widespread belief in our country that some socially good things derive from the current inability to strongly correlate an identity with an individual—for example, a person often has the option of leaving some detail of his or her life behind. Examples include the expunging of the criminal records of minors, anonymous testing for sexually transmissible diseases (and the consequent public-health benefits of reducing the incidence of these diseases), shielding the identity of rape victims from public view, and erasing the records of bankruptcy after a statutory interval.

It is not known how much the smooth operation of society depends on such things, or on the assumption that they are possible. There is a risk, however, that they would be lost, or at least significantly impaired, if a broadly used nationwide identity system came into existence.[26] Ensuring the privacy protections in these examples would likely depend on carefully limiting access to, and the specific uses of, the system's databases, and on restricting the required uses of an ID to certain circumstances.

[25] Garrett Hardin, "The Tragedy of the Commons," *Science*, 162, 1243-1248 (1998).

[26] Years of experience show that when people automate or regiment a previously manual or only lightly regimented system, they discover the new system's demand that things be done "exactly right" can create havoc, and that what used to be a smooth process needs to be redesigned to accommodate the less flexible automated system. Decision makers must consider that introducing a rigorous identity system might wreak similar havoc when people discover that some authentication activities require more flexibility than the new system can offer.

http://www.nap.edu/openbook/0309064309/html/23.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

Identity theft is already a critical problem,[27] even without centralized, mandated identities for everyone. Identity theft is an individual's fraudulent claim that he or she is the person to whom information in the system refers, consequently deriving some benefit from another party who is relying on that claim. It might involve theft of a physical ID token or it might involve the thief's learning some secret or personal information and using this in lieu of the token. One reason for the problem is the broad misuse of SSNs, coupled with the fact that the number itself is small enough to be easily memorized. In addition, birth and death data in the United States are not subject to stringent accuracy requirements nor are they highly correlated, making it relatively straightforward to exploit a deceased person's birth certificate in order to establish credentials as a basis for an identity.

Given the attendant risks, a nationwide identity system would need to provide much better protection against identity theft than do current systems of identification.[28] Additional questions arise in the context of a nationwide system of how to recover from identity theft. Who would have the authority to restore or create a new identity for someone when necessary? And what safeguards would be needed to prevent this authority from being abused?

While offering better solutions to some problems surrounding identity theft, a nationwide identity system poses its own risks. For example, it is likely that the existence of a single, distinct source of identity would create a "single point of failure" that could facilitate identity theft. The theft or counterfeiting of an ID would allow an individual to "become" the person described by the card, in very strong terms, especially if the nationwide identity system were to be used for many purposes other than those required by the government. Paradoxically, it could be that a robust nationwide identity system makes identity theft more difficult while at the same time making its consequences more dire. The economic incentive to counterfeit these cards could turn out to be much greater than the economic incentive to counterfeit U.S. currency.

To determine what safeguards are necessary, a realistic threat analysis would be required. Are the as-yet-undetermined countermeasures up to the challenge? Any proposed system must be examined to determine whether the net result with respect to identity theft would be better or worse than it is now. It may be that more robust security in a nationwide identity system, along with increased attention to data integrity (for example, correlating birth and death records, as discussed above) in current identity systems, would mitigate some of the identity-theft problems that arise.

[27] *Time* notes that in 2001 the "Federal Trade Commission logged more than 85,000 complaints from people whose identities had been pirated" and that "some consumer advocates suggest as many as 750,000 identities are stolen each year." See <http://www.time.com/time/nation/article/0,8599,196857,00.html>.

[28] One strategy might be for the system to avoid displaying human-readable ID "numbers" or other unique identifiers to private organizations. This would, in effect, make it impossible for anyone to read another person's information off his or her card. (Imagine, for example, a credit card that does not have the account number embossed on the front, but that makes it available only to machines that read magnetic stripes, thereby reducing opportunities for casual theft). The strategy would instead require that agents use cryptographic techniques to authenticate individuals or enable transactions. See Figure 2.1 for a description of the kinds of information in an identity system and where the information might end up.

http://www.nap.edu/openbook/0309084393/html/24.html, copyright , 2001 The National Academy of Sciences. all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

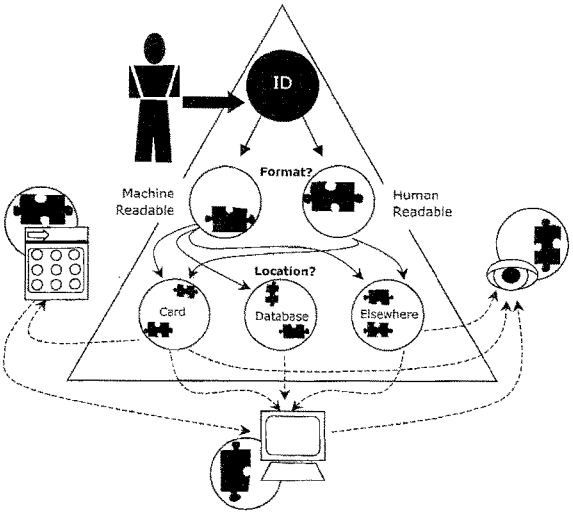


FIGURE 2.1 Potential information flow in identity systems.

The information associated with an individual identity could be distributed within the identity system in multiple ways. Parts of it may be machine-readable, parts may be readable by humans. Parts may be stored on a card, in a database, or elsewhere. Access to this information may be available to other systems, card readers, and/or people. Not present in this diagram, but implicit, is the notion that pieces of information, once outside the system, could then be added to other systems. Or, information from outside the system could be incorporated into this system.

http://www.nap.edu/openbook/0309084830/html/25.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

3 Technological Challenges

Though the aim of this short report is merely to point out some of the essential policy questions that would be raised by the introduction of a nationwide identity system, the committee believes that the technological and implementation challenges raised—even without a precise characterization of such a system's goals or subsequent policies—are enormous and that they warrant significant and serious analysis.

This need becomes clear when an ID is understood as an element of a much larger system, that includes technical, material, and human elements. At a minimum:

- Cards and card readers (if used for validation) would need to be designed, fabricated, distributed, and updated or otherwise maintained or replaced.
- A corresponding (backend) database would need to be established, maintained, and protected.
- Procedures for checking the authenticity of IDs and for verifying the presenter (with or without specialized equipment) would need to be established, promulgated, practiced, and audited.[1]
- Means to discover, report, verify, and authoritatively correct mistakes would need to be put into place.
- A variety of security measures would need to be factored into all aspects of the system to be sure that it meets its objectives and is not vulnerable to things such as fraud or denial-of-service abuses that can result in privacy violations.

Fraud (and security in general) is a significant concern in any system, even the most technologically sophisticated.[2] The nationwide scale of such a system would require knowing that all aspects of the system are scalable—a daunting problem for lesser systems.[3] In any case, the challenges of building robust and trustworthy information systems—they are extensive and well-documented[4]—are only accompanied by the even greater challenge of making the systems resistant to attacks by well-funded adversaries.

Architectural issues include the degree of centralization of the underlying databases as well as the location and cost of data storage, computation, and communication, which can all be done at different

[1] Association of an identity card with its holder has to be verified before the identity information it contains can be relied upon (otherwise stealing the card would permit the theft of the cardholder's identity).

[2] A large breach of security with the French banking cards is causing a significant upgrade of the infrastructure in France (<http://parodie.com/english/smartcard.htm>). In the United States, satellite-signal theft by smartcard fraud is so extensive that it is now the focus of a government sting operation. See Ross Anderson's work on cryptography and security, much of which is available at <http://www.cl.cam.ac.uk/users/rja14/>.

[3] CSTB's 2000 report *Making IT Better* underscores the profound challenges associated with large-scale systems.

[4] See the CSTB reports *Computers at Risk* (1990), *Trust in Cyberspace* (1999), *Making IT Better* (2000), and *Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers* (2001).

http://www.nap.edu/openbook/0309088437/html/26.html, copyright, 2001 The National Academy of Sciences, all rights reserved.

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

places.[5] For example, would authorized entities obtain the records they wanted, under what circumstances, and with what degree of authorization? Would there be daily or weekly downloads of selected records to more permanent storage media? Would a real-time network feed be required (perhaps similar to those used in real-time credit authorization systems)? Would it be possible to secure such a feed sufficiently?[6]

Choices among architectural options, as well as other options, would depend on the functional goal(s) of the system. Architecture influences scalability, cost, and usability/human factors. It also interacts with procedure: Decisions must be made about who would be in charge of issuing, reissuing, renewing, revoking, and administering the cards, along with maintaining, updating, and granting access to the database. A further concern is the need for graceful recovery from failure as well as substitute mechanisms when the system is compromised or not adequately responsive at the time verification of an identity is needed. All of these factors influence cost, as well as effectiveness.

Cost needs to be analyzed completely, on a life-cycle basis and with attention to numerous tradeoffs. Even if software and hardware costs are minimized, experience with lesser systems—from SSNs to state drivers' licenses to military identification systems—shows that there will be significant ongoing administrative costs for training, issuing cards, verification, maintenance (keeping whatever information is associated with an individual and his or her ID up to date), and detection and investigation of counterfeiting.[7] In particular, the costs—and technological and administrative complexity—of assuring the integrity and security of an identity infrastructure are likely to be large. They would depend in part on whether technology for automated checking of an ID—as opposed to a visual check used today with SSNs or drivers' licenses—is required, which in turn depends on the choice of ID technology (see Box 3.1).

For example, in response to legislation enacted in August 1996,[8] the Social Security Administration (SSA) conducted an analysis and produced a report on options for enhancing the Social Security card.[9] Citing a number of key business and technology assumptions that appeared valid at the time of the study (1997), SSA estimated that issuing enhanced cards might have a life-cycle cost of $5.2 billion to $10.5 billion, depending on the technology developed and deployed. These estimates included assumptions about the need for reissuing cards, issuing new cards, and maintaining the systems in order to store data related to the cards and keep that data current and up to date. This study did not assume that each SSN and its related card would relate to just one individual, as SSA estimated that at the time, approximately 10 million of the 269 million SSNs valid were duplicates (that is, two or more persons had been given the same SSN). There was a variety of reasons for such duplication, including error on the part of SSA and malfeasance on the part of some individuals.

As with the design of any system, decisions about tradeoffs would need to be made in advance. The security, efficiency, and effectiveness options chosen would depend on the goals and policies

[5] A general rule is that the lower the cost of accessing an online database and the larger the likelihood of doing so, the less sophisticated the card needs to be.

[6] Such security might require a very large new network that would have to be connected *inside* the firewalls of the institutions and organizations using the system. Securing such a network is extremely difficult; experience suggests that maintaining that security would be very challenging.

[7] There are numerous ways in which fraudulent ("novelty") identification documents can be obtained. A simple Web search on "fake id" provides links to many possible suppliers.

[8] Section 111 of P.L. 104-193, "Personal Responsibility and Work Opportunity Reconciliation Act of 1996" (Welfare Reform) and section 657 of P.L. 104-208, Division C, "Illegal Immigration Reform and Immigrant Responsibility Act of 1996" (Immigration Reform).

[9] See *Report to Congress on Options for Enhancing the Social Security Card*, Social Security Administration SSA Publication No. 12-002, September 1997 at <http://www.ssa.gov/history/reports/ssnreport.html>.

http://www.nap.edu/openbook/0309084830/html/27.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

(see Chapter 2) and the planned uses of the system. For example, a "trusted traveler" system, whose sole function was to authenticate individuals who had been previously certified as "trusted" in the particular context of travel, might place more emphasis on efficiency in travel-related lines and eliminating false positives than on protecting the fact that a particular person has been certified as trusted (or untrusted). A secure driver's license system, in which the license is used as an ID for many activities beyond driving on a public roadway, may trade ease of replacing a lost license against the rigorous authentication of individuals who request a replacement. In making decisions about trade-offs, understanding the potential threats and risks will be a large component of assessing the security requirements of a system.

BINDING PERSONS TO IDENTITIES

A practical issue that would arise in a card-based identity system is that of relating cards and identities to individuals: How would the issuing authorities create this binding? Most of the systems (both hypothetical and actual) alluded to in this report employ what is known as two-factor authentication, requiring the holders to present more information than the card itself (perhaps a face that matches the picture, a PIN, or a thumbprint) to verify that they are the legitimate holders.

If someone has a valid card, how would anyone know that it belongs to him or her? A picture on the front of the card would not be sufficient if very high assurance is sought.[10] If the card makes use of a magnetic stripe, it would have been easy to copy the stored information to a new card with a different picture. If the card is a memory card or smart card, duplication, while a little more difficult, would still have been possible. If biometric information[11] is used, it could have been stored on the card and a "live capture" of the biometric could be carried out when an individual presents the card. The captured data would then be compared with the data stored on the card. Depending on what kinds of cryptographic protections were used, this system could be susceptible to forgery as well—for example, someone might recreate the card with his or her own biometric information in combination with another person's identity information.

Another scenario might be to have the person present a biometric to a controlled scanner, and present the card that contains reference information. Both pieces of information are then validated in combination against a backend server. However, this creates a requirement for high availability (that is, the system should be usable essentially all of the time) and a dependence on reliable, secure network and communications infrastructures.

In principle, a card coupled with biometrics and the appropriate infrastructure for reading and verifying biometric data may offer the greatest confidence with respect to linking persons and their cards. But getting biometrics technology right (including control of the risks of compromise) and widely distributed is not easy.[12,13] There are additional issues associated with the use of biometrics, such as some popular resistance.[14]

[10] The inability of human inspectors to reliably match faces to cards was demonstrated in Pike, Kemp and Brace, "Psychology of Human Face Recognition," IEEE Conference on Visual Biometrics, March 2, 2001, Savoy Place, London.

[11] There are number of biometrics that might be used; for the purposes of this discussion, assume an iris scan or fingerprint.

[12] "Advice on the Selection of Biometric Products: Issue 1.0," (U.K.) Communication Electronic Security Group, 23 November, 2001, as available at <http://www.cesg.gov.uk/technology/biometrics>.

[13] J.D.M. Ashbourn, *Biometrics: Advanced Identify Verification: The Complete Guide*, Springer, London, 2000.

[14] For further information, see the recent RAND report, *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns*, 2001. In addition, an accuracy issue arises with biometrics because it uses what are known as probabilistic measures of similarity. No two images of the same biometric pattern (even

http://www.nap.edu/openbook/0309084203/html/28.html, copyright . 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

Note that biometrics allows for cardless system options: A database-only system based solely on biometrics eliminates the risk of card loss or theft, but real-time database accessibility then becomes a major consideration. In addition, compromise of the database is an even greater concern than in card-based systems, where the cards can be used to provide a check against corrupted data in the database. Further, a cardless system implies that anyone wishing to use the system (even for activities needing only moderate to low levels of security) would have to invest in the equipment needed to access the infrastructure in real time.

Cryptographic protection and digital signatures, in combination with offline verification of the signature and a properly deployed public key infrastructure (PKI),[15] could provide a measure of protection for the information associated with IDs and guard against misuse. But for any technology, some degree of imperfection will exist. Therefore, it is necessary to decide on thresholds for false rejection rates (false negatives) and false acceptance rates (false positives), not only for when the ID is used but also at the time of issuance, reissuance, and renewal. Policy decisions—perhaps with corresponding legal backing—need to be made about what happens in the event of a false negative or false positive. Creation of exception-handling procedures for dealing with incorrect decisions opens up additional vulnerabilities for the system, as impostors might claim to have been falsely rejected and request handling as an exception.

BACKEND SYSTEMS

Once methods are in place to satisfactorily link persons to IDs, the requirements and goals of the system should drive decision-making about associated databases. The databases' principal features are likely to include an ability to search based on an ID number or other unique identifier, various ID attributes, and possibly biometric data. Depending on whether tracking and prediction are requirements of the system, significant logging, auditing, and data mining capabilities would be needed as well.

Key issues related to this part of the system stem from both structural and procedural decisions. If the database needs to be readily accessible from remote locations (which is likely), it would almost certainly need to be replicated. This, in combination with its perceived (and actual) value and the fact that more people over a more widespread area would be likely to have authorized access to the system, makes it even more vulnerable to break-ins: by physically accessing one of the sites, by finding some communications-based vulnerability, or by bribing or corrupting someone with access to the system. Moreover, if verification of identity required an online database query at airports, a handful of "accidents" at key places around the country (such as wires being cut at critical points in a way that appears accidental) could cripple civil aviation and any other commerce that required identity verification (for example, purchase of guns or certain chemicals).

Note that availability would be a key aspect of any online component of a nationwide identity system. While the desire for cost savings might lead to such a backend system being accessible via the public Internet (as opposed to a dedicated network), this would expose the system to yet more attacks, both direct and indirect, on shared infrastructure, such as the routing systems and hardware, the domain name system, or shared bandwidth. As noted previously, it has proven extremely difficult to secure systems that utilize the Internet; a nationwide identity system would likewise need to be widely accessible and would inevitably be the target of malicious attacks as well as subject to

---

fingerprints) from the same person are exactly alike. Consequently, biometrics is based on pattern-matching techniques that return sufficiently close measures of similarity. With enough (or not enough) information about the application environment and user population, it is possible to convert those measures into probabilities of a match or nonmatch. Thus, incorrect decisions occur randomly with a probability that can be measured.

[15] The committee's final report will examine PKI and other authentication technologies in detail.

http://www.nap.edu/openbook/0309068304/html/29.html, copyright 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

unintentional or incidental damage. Failure modes of the system would have to be very carefully studied, and backup plans and procedures would have to be designed and tested for all critical systems that depend on use of the nationwide identity system.

A further complication would result if it were decided that different users be granted different levels of access to the database, whether for aggregated data or information about individuals. This raises query capability, access control, and security issues. Related to the size of the user base (that is, those who use the identity system to make some sort of determination about an individual) is the question of whether the same security measures need to hold for each user. For example, if the system were used broadly in the private sector, a clerk at a liquor store might be relatively less concerned about detecting counterfeit cards than would be an intelligence or law enforcement agent granting access to national security-related sites or information. In addition, the clerk would need less information (for example, age of individual is greater than 21) verified through the system than would the agent.

It is a significant challenge to develop an infrastructure that would allow multiple kinds of queries, differing constraints on queries (based on who was making them), restrictions on the data displayed to what was needed for the particular transaction or interaction, and varying thresholds for security based on the requirements of the user. Determining the scope of use and the breadth of the user population in advance would dictate whether this was necessary.

A further challenge resulting from a wide variety of users and uses is data integrity. Different users (even if the system were used only by agencies within the government) would undoubtedly have different perceptions of how critical the accuracy of the data is. Therefore, to maintain the quality of the data, controls over who could input data and with what degree of specificity and security must also be a factor in the design of the system.

Another necessary component of system and data integrity is auditing capability. Keeping track of who has accessed what parts of the system and which data would be necessary both for reasons of technology (to track down errors and bugs, for example) and liability.[16]

Procedurally, such a large system would require many people to be authorized to maintain and administer it. Even if perfect technological security were achievable, there would still be the security risk of compromised insiders, given the very large numbers of people needed to maintain and administer the system.[17,18] The human factor would also be an issue with regard to data entry and possible errors in the database. This is well known among statisticians, and various technical and procedural steps can be taken to offset risks of inaccuracy. In general, therefore, correction mechanisms would need to be created; however, these mechanisms provide additional opportunity for fraud. Given the uses to which such a system is expected to be put, though, and potential impacts on individuals' reputations and freedom to function as social and economic actors, mechanisms that allow individuals to know what is in the database and to contest and/or correct alleged inaccuracies would be desirable and politically essential, (and, if run by the federal government, legally required).

---

[16] Indeed, major federal agencies such as the Internal Revenue Service have run into problems with respect to tracking and controlling access to information. For a discussion of this as it relates to privacy, see Peter P. Swire, "Financial Privacy and the Theory of High-Tech Government Surveillance," *Washington University Law Quarterly*, 177(2):461-512 (1999).

[17] CSTB held a planning meeting on the topic of the insider threat in late 2000. For more information, see <http://www.cstb.org/web/whitepaper_insiderthreat>.

[18] The President's Commission on Critical Infrastructure Protection at <http://www.ciao.gov/PCCIP/PCCIP_Report.pdf> discusses cyberthreats, including the insider threat. *Fortune* has examined the cost of insider attacks online at <www.fortune.com/sitelets/sections/fortune/tech/2001_01esecurity2.html>.

http://www.nap.edu/openbook/0309084030/html/30.html, copyright 2002 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

While such mechanisms can be found in credit-reporting and medical databases,[19] the law-enforcement and national-security frameworks that are motivating proposals for a nationwide identity system pose unique accessibility and disclosure challenges.

Another concern is that depending solely on feedback from participants to correct inaccuracies would catch only a fraction of the errors. People may tend to notice and report only those errors that interfere with something they are attempting to accomplish. An incorrectly entered birth date, for example, may not be noticed or corrected for decades and may only come to light when the person applies for, say, Medicare. An accumulation of latent errors is inevitable and leads to at least two problems: (1) by the time the error is discovered it may be hard to locate the information needed to verify the claim of error and (2) the act of making the correction may interfere with or delay some action that should be allowed by the system. Creating a workable nationwide identity system that can compensate in effective ways for these inevitabilities is clearly a nontrivial task.

DATA CORRELATION AND PRIVACY

A key question about a nationwide identity system database is whether it would be designed to foster consolidation of other (especially federal) databases—or whether that might happen as a side effect. Either way, proponents note that this would make information sharing among intelligence and law enforcement agencies easier,[20,21] although the committee believes that it could also carry significant risks.

A centralized, nationwide identity system essentially offers adversaries a single point of failure and presents an attractive target for identity theft and fraud. The more valuable the information in the database and the credentials associated with an identity, the more they become a target for subversion. Unauthorized access might be sought by terrorists, stalkers, abusive ex-spouses, blackmailers, or organized crime. Furthermore, to the extent that important activities become dependent on the system, the system becomes an attractive target for denial-of-service attacks. Implementing a secure and reliable nationwide identity system that is resistant to credential theft or loss,[22] fraud, and attack is a significant technological challenge, with ancillary procedural challenges.

Related to consolidation, information *correlation* is facilitated by systems in which one individual has exactly one identity. This has both negative and positive implications. Such a system is useful for predicting or detecting socially detrimental activities, because it avoids the uncertainty and confusion that may arise from multiple identities (notwithstanding that multiple identities can serve useful and socially desirable purposes, as described previously). Credit card companies, for example, can conduct behavior-pattern analysis for fraud detection.[23] Similar technologies must be

[19] See, for example: Computer Science and Telecommunications Board. 1997. *For the Record: Protecting Electronic Health Information*, National Academy Press, Washington, DC.

[20] A forthcoming CSTB report will explore issues on critical information infrastructure protection and the law, including a preliminary analysis of the issue of information sharing between the public and private sectors. For more information see <http://www.cstb.org/web/project_cip>.

[21] See, for example, Larry Ellison's October 8, 2001 article in the *Wall Street Journal*, "Digital Ids can Help Prevent Terrorism", and Cara Garretson's December 2001 article in *CIO*, "Government Info Sharing Key to Fighting Terrorism" <http://www.cio.com/government/edit/122001_share.html>.

[22] Loss of ID cards presents its own challenges to the system; if all of the individuals with lost IDs were to become immediately "suspect" in the system, intolerable backlogs and/or overload could result.

[23] Credit card companies make these correlations using both standard statistical methods and neural networks. More information can be found at <http://www3.autodesk.com/adsk/item/0,,280162-123112,00.html>.

http://www.nap.edu/openbook/0309084,00X/html/31.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

used to detect behavior indicative of impending criminal or terrorist activities, although this raises concerns about profiling.

On the negative side, such analysis also enables invasions of personal privacy. The extent to which this occurs would depend heavily on the circumstances under which an individual can be compelled to present an ID, what information is retained, and which activities are tracked within the system (a topic explored above). Indeed, detecting a problem might only be possible in some instances through broad analysis. This would necessitate examining the behavior of many people who do not pose a risk—most human behavior involves law-abiding citizens pursuing Constitutionally protected activities—in order to identify the few who do.[24]

[24] For a discussion of some of the effects and implications of ubiquitous surveillance cameras, see the October 7, 2001, article by Jeffrey Rosen, "A Watchful State," *New York Times Magazine.*

http://www.nap.edu/catalog.php?record_id=10867#toc Copyright © 2001 The National Academy of Sciences. All rights reserved.

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

BOX 3.1
Cards and Their Requirements

The presumed goal of a counterfeit-resistant, long-lasting, easily replaceable ID presents difficult technical challenges. With respect to the ID itself, assuming that it is a physical artifact such as a card, a number of questions need to be answered. Form factors—the size, shape, and substance of the card—would likely play a part both in acceptance on the part of the citizenry and in the card's resistance to counterfeiting. The more difficult challenges pertain to the aspects of cards that are determined by the kind of technology used.

One could use a relatively simple card, like a credit card or drivers licenses. Each individual in the system would have a card with some information printed on it about the holder, and perhaps a picture. There might be a unique number on the card, and the information in a nationwide database would be indexed by that number. The card itself might contain a magnetic stripe along with embossed and printed data. As with a driver's license or passport, access to the database (for reading data out or putting data in) would presumably be limited. A system like would be underlie proposals by the American Association of Motor Vehicle Administrators to create national standards for drivers licenses.

On the other hand, the counterfeiting of magnetic stripe cards is a [illegible]. More important, the ease with which the information contained in the magnetic stripe can be duplicated means that a counterfeiter can produce a blank card and rewrite on the data in the transactions as if the card came from a genuine card. A lot of the implications for security and privacy, vulnerabilities, and the like are equally true of systems that rely on biometrics such as [illegible] between the holder of the card and the person to whom the card was issued. Further, using such credentials as a basis for issuing new cards could lead to identity compromise, the acceptance of some of the identification documents as the determination by the individual or even third parties.

Another possibility is a [illegible] card that would [illegible] information and be more [illegible] than magnetic stripe cards, but also more expensive. These cards contain [illegible] some [illegible] that is [illegible] reading or tampering with the card. The information contained [illegible] digitally signed by [illegible] number could be associated with [illegible] on the card [illegible] with the information on the card and [illegible] [illegible] on the card [illegible] with the information on the card and [illegible] [illegible] [illegible]

Copyright © National Academy of Sciences. All rights reserved.

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

As an example of a card-based system using biometrics, consider the Connecticut Department of Social Services, which issues cards to aid welfare recipients.[6] Fingerprints of each applicant are taken and compared to the fingerprint of all applicants previously enrolled. Under the assumption that people are not modifying their fingerprints (and assuming no matching errors), this can prevent a single user from registering under multiple identities within the system. The card is printed with the fingerprints encoded in a two-dimensional optical bar code on the front of the card. At point-of-service applications, the user presents a fingerprint that is compared with that encoded on the card. This prevents multiple users from making use of a single identity. Other biometric technologies, such as iris recognition, might be useful in this application as well. However, no biometric technology is completely invulnerable to attacks by sophisticated adversaries.[7,8]

---

[1] The Department of Defense is now deploying a smartcard that it refers to as a Common Access Card (CAC)—as an authentication device and for other purposes, the card combines a magnetic stripe, bar code, a photo ID, and smartcard technology. DOD's experience may well prove instructive when considering a nationwide system. However, the privacy concerns of military employees are likely to be different from those of average citizens, making an exact analogue unlikely. In addition, the CAC will be deployed for a population that is more than an order of magnitude smaller than the U.S. population, which is more diverse in many dimensions than the military, and which is currently less subject to sanctions for failure to comply with the identification system's requirements.

[2] On November 2, 2001, the *Washington Post* reported that the American Association of Motor Vehicle Administrators was working on a plan to link all driver databases and to strengthen the security and functionality of current drivers licenses and state identification cards. See <http://www.washingtonpost.com/wp-dyn/articles/A32717-2001Nov2.html>. See also <http://www.aamva.org/standards/stdAAMVADLIstandard2000.asp> for a description of the Association's standard, which aims to provide a uniform means for identifying holders of drivers licenses throughout North America.

[3] See, just as two of many examples, "Scam Artists Can Swipe Your Credit," <http://www.techtv.com/cybercrime/internetfraud/story/0,23008,2383624,00.html>, and "Newly Discovered Bug Skims Credit Card Data," <http://www.newsfactor.com/perl/story/14494.html>.

[4] Note that the existing identification infrastructure (including the system of birth and death records) in the United States often depends on the presentation of credentials under a highly decentralized. The lack of common national standards generates skepticism about the quality of the data.

[5] One example is the INSPASS and the data stored on it, combined with a hand geometry reader at point of entry to verify identity. Another example is a German identification card, the *Geldkarte*, which uses two separate smartcard chips and contains 22 separate mechanisms to thwart value and antifraud technology.

[6] For a discussion of the costs associated with identification cards and fingerprints in social service applications, see "A Review of Five Cost/Benefit Studies of Fingerprinting in Social Service Applications," Roger Stanton, Burton Turkel, and James Wayman, available at <http://www.biss.state.ct.us/inc/al/news22/ons/n22.htm>.

[7] T. van der Putte and J. Keuning, "Biometrical Fingerprint Recognition: Don't Let Your Fingers Get Burned," *Proceedings of IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications*, Kluwer Academic Publishers, September 2000, pp. 289-303. Also, See T. Matsumoto, et al., "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems," *Proceedings of the SPIE*, Vol. 4677 (January 2002), and D. Maio, D. Maltoni, J. L. Wayman, and A. Jain, "FVC2000: Fingerprint Verification Competition," *Proceedings of the 15th International Conference on Pattern Recognition*, Barcelona, September 2000. Available online at <http://bias.csr.unibo.it/FVC2000/>.

http://www.nap.edu/openbook/0309084830/html/34.html, copyright 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

[PAGE INTENTIONALLY LEFT BLANK]

http://www.nap.edu/openbook/0309064309/html/35.html, copyright 2001 The National Academy of Sciences, all rights reserved.

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

4 Concluding Remarks

Given the complexity of a nationwide identity system, its potential impacts, and the broad scope of the issues it raises, the committee believes that much more analysis is needed. Such analysis cannot proceed, however, without a clear articulation of the system's goals and requirements. The committee believes that if a nationwide identity system is to be created, the goals of such a system must be clearly and publicly identified and deliberated upon with input sought from all stakeholders (including private citizens). Given the economic costs, the significant design and implementation challenges, and the risks to security and privacy posed by a poorly thought-out system, prior public review[1] is essential.

Thus the committee believes that proponents of a nationwide identity system should be required to present a very compelling case addressing these issues and that they should solicit input from a broad range of stakeholder communities.[2] The committee's own discussion of a nationwide identity system, although brief and modest in scope, raised numerous complex questions. It is clear that an evaluation of the potential costs, presumed benefits, and potential drawbacks of any proposed system is necessary in order to fully appreciate its trade-offs.

Care must be taken to completely explore the ramifications of any nationwide identity system not only because of the significant policy concerns and technological challenges but also because after-the-fact costs—the result of revoking, correcting, or redesigning after broad deployment—would be enormous. Moreover, analysts must give serious consideration to the idea that—given the broad range of potential uses, security requirements, and privacy needs that might be contemplated—no single nationwide identity system is likely to meet the varied demands of all potential users. Undoubtedly many more issues exist that are not even touched upon here.

Given the wide range of technological and logistical challenges, the likely direct and indirect costs, the serious potential for infringing on the rights and freedoms of ordinary citizens, and the gravity of the policy issues raised, any proposed nationwide identity system requires strict scrutiny and significant deliberation well in advance of design and deployment.

---

[1] For an example of how this might work, consider the public-review cycle for the Advanced Encryption Standard (AES); see <http://csrc.nist.gov/encryption/aes/>, managed by the National Institute of Standards and Technology.

[2] Other stakeholder groups have already commented on the idea of a national identity card, albeit within varying contexts. For example, in 1995 the Cato Institute presented an extensive policy analysis of the notion of a nationwide worker registry within the context of a larger immigration debate (see <http://www.cato.org/pubs/pas/pa237.html>). The American Civil Liberties Union offered similar opposition (see <http://www.aclu.org/library/aaidcard.html>); and around the same timeframe, Privacy International prepared a report describing the use and implications of national ID cards from an international perspective (see <http://www.privacy.org/pi/activities/idcard/idcard_faq.html>).

http://www.nap.edu/openbook/0309084303/html/37.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

Appendix A

Committee Member and Staff Biographies

STEPHEN T. KENT, *Chair*, is chief scientist for information security at BBN Technologies, a division of Verizon Communications. During the last two decades, Dr. Kent's R&D activities have included the design and development of user authentication and access control systems, network layer encryption and access control systems, secure transport layer protocols, secure e-mail technology, multilevel secure (X.500) directory systems, and public-key certification authority systems. His most recent work focuses on security for Internet routing, very high-speed IP encryption, and high assurance cryptographic modules. Dr. Kent served as a member of the Internet Architecture Board (1983-1994) and chaired the Privacy and Security Research Group of the Internet Research Task Force (1985-1998). He chaired the Privacy Enhanced Mail (PEM) working group of the Internet Engineering Task Force (IETF) from 1990 to 1995 and co-chairs the Public Key Infrastructure Working Group (1995-present). He is the primary author of the core IPsec standards: RFCs 2401, 2402 and 2406. He is a member of the editorial board of the *Journal of Computer Security* (1995-present), serves on the board of the Security Research Alliance, and served on the board of directors of the International Association for Cryptologic Research (1982-1989). Dr. Kent was a member of CSTB's Information Systems Trustworthiness Committee (1996-1998), which produced *Trust in Cyberspace*. His other previous NRC service includes the CSTB Committee on Rights and Responsibilities of Participants in Networked Communities (1993-1994), the Technical Assessment panel for the NIST Computer Systems Laboratory (1990-1992), and the CSTB Secure Systems Study Committee (1988-1990). The U.S. Secretary of Commerce appointed Dr. Kent as chair of the Federal Advisory Committee to Develop a FIPS for Federal Key Management Infrastructure (1996-1998). The author of two book chapters and numerous technical papers on network security, Dr. Kent has served as a referee, panelist, and session chair for a number of conferences. Since 1977 he has lectured on the topic of network security on behalf of government agencies, universities, and private companies throughout the United States, Europe, Australia, and the Far East. Dr. Kent received the B.S. degree in mathematics, summa cum laude, from Loyola University of New Orleans and the S.M., E.E., and Ph.D. degrees in computer science from the Massachusetts Institute of Technology. He is a fellow of the ACM and a member of the Internet Society and Sigma Xi.

MICHAEL ANGELO is currently a staff fellow at Compaq Computer Corporation and runs a laboratory at Compaq that assesses biometrics and other security-enhancing technologies, such as smart cards. He is considered a subject-matter expert for security and its associated technologies. His job is to provide technical guidance and input into strategic planning and the development of secure solutions. In addition, he is responsible for providing technical assistance to the corporate security team. Dr. Angelo possesses expertise in both biometric and token access authentication technology, including technical threat model and implementation analysis, as well as in risk reduction enhancement methodology, applied computer system security, computer forensics, advanced data protection methodologies, and practical encryption techniques. His experience comprises 15 years in designing, implementing, managing, and supporting secure intra- and Internets, including gateways, firewalls, and sentinels, plus 20 years working at the kernel level of numerous operating systems, including a wide variety of hardware platforms (from PCs to supercomputers) and software platforms (including several flavors of UNIX, MS-DOS/Windows/NT, and VMS). He holds several patents. Dr. Angelo has been active in a

http://www.nap.edu/openbook/0309084300/html/38.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

number of trade standards organizations: the Trusted Computing Platform Association (TCPA), Americans for Computer Privacy (ACP), the Bureau of Export Administration Technical Advisory Committee (BXA-TAC), the Information Security Exploratory Committee (ISEC), the Key Recovery Alliance (KRA), the Computer Systems Policy Project, the Cross-Industry Working Team Security Working Group, and the National Institute of Standards and Technology's Industry Key Escrow Working Group.

STEVEN BELLOVIN is a Fellow at AT&T Research. Dr. Bellovin received a B.A. degree from Columbia University and an M.S. and Ph.D. in computer science from the University of North Carolina at Chapel Hill. While a graduate student, he helped create Netnews; for this, he and the other collaborators were awarded the 1995 USENIX Lifetime Achievement Award. At AT&T Laboratories, he does research in networks and security, and why the two do not get along. Dr. Bellovin has embraced a number of public interest causes and weighed in (e.g., through his writings) on initiatives (e.g., in cryptography and law enforcement) that appear to threaten privacy. He is currently focusing on cryptographic protocols and network management. Bellovin is the co-author of the recent book *Firewalls and Internet Security: Repelling the Wily Hacker*, and he is a member of the Internet Architecture Board. He was a member of the CSTB committee that produced *Trust in Cyberspace* (1999) and he is a member of the National Academy of Engineering.

BOB BLAKLEY is chief scientist for security and privacy at IBM Tivoli Software in Austin, Texas. Dr. Blakley was chief scientist for DASCOM, Inc., at the time of its acquisition by IBM and integration into Tivoli. Before joining DASCOM, Dr. Blakley was lead security architect for IBM, where he was employed for 9 years. In addition to his product design responsibilities, Dr. Blakley led the IBM Security Architecture Board and was the IBM representative to the Open Group Security Program Group. He also served for 2 years as the chair of the OSF DME/DCE security working group. He is the author of *CORBA Security: An Introduction to Safe Computing with Objects*, published by Addison-Wesley. Dr. Blakley was also the editor of the Open Group PKI working group's "Architecture for Public Key Infrastructure." Dr. Blakley has been involved in cryptography and data security design work since 1979 and has authored or coauthored seven papers on cryptography, secret-sharing schemes, access control, and other aspects of computer security. He was designated "Distinguished Practitioner" by the 2001 Annual Computer Security and Applications Conference. He is currently the general editor of the OASIS Security Services Technical Committee's SAML specification effort. He holds eight patents on security-related technologies. Blakley cochaired the ACM New Security Paradigms Workshop in 1997 and 1998, and he served on the program committees for several industry and academic conferences, including the NSA/OMG Distributed Object Computing Workshop, IEEE Security and Privacy, and ISOC Network and Distributed Systems Security (NDSS). Dr. Blakley received an A.B. in classics from Princeton University and a master's degree and Ph.D. in computer and communications sciences from the University of Michigan.

DREW DEAN is a computer scientist at SRI International. While a student at SRI International, he developed a formal model of dynamic linking with static typing in Java-like environments. He also tackled first-class environments in a statically typed language and consulted on intrusion detection. Dr. Dean builds on work on Java security at Princeton University, and he has been involved with the Secure Digital Music Initiative and other activities that relate to protection of intellectual property. His activities have focused him on understanding how systems work or do not relative to their stated goals. Dr. Dean earned a B.S. with honors in mathematics and computer science from Carnegie Mellon and an M.A. and Ph.D. in computer science from

http://www.nap.edu/openbook/0309084301X/html/39.html, copyright , 2001 The National Academy of Sciences, all rights reserved

Princeton University. Dean has written several papers, and he is associate editor of the *Information Journal of Information Security*. He is a member of ACM and IEEE.

BARBARA FOX is currently senior architect, Digital Rights Management and Cryptography, at Microsoft Corporation. She is coauthor of a number of research papers in the application of public key infrastructures to payment systems and, most recently, the IETF/W3C XML Digital Signature standard. Ms. Fox also serves on the board of directors for the International Financial Cryptography Association.

STEPHEN H. HOLDEN is an assistant professor in the Department of Information Systems at the University of Maryland Baltimore County (UMBC). Dr. Holden's research, publications, and teachings leverage his substantial federal government experience in government-wide policy in information technology management and electronic government. Other research interests include information policy, electronic authentication policies and practices, and strategic management processes. He recently left the Internal Revenue Service (IRS) as a senior executive after a 16-year career in the federal career service. While at the IRS he served as the program executive, Electronic Tax Administration (ETA) Modernization, reporting to the assistant commissioner (ETA). Before that position in ETA he served as the national director of Electronic Program Enhancements. During that time he led efforts to develop new ETA programs, policies, and e-government systems for the IRS, including the ETA partnership effort, electronic payments, electronic authentication, and the IRS e-file promotional campaign. He also served on the federal Public Key Infrastructure Steering Committee. Prior to going to IRS, Dr. Holden worked for 10 years at the Office of Management and Budget (OMB), doing a variety of policy, management, and budget analysis work. Significant accomplishments at OMB included drafting and completing a revision to the information technology management section of Circular A-130 and overseeing the publication of the first "Information Resource Management Plan of the Federal Government." Dr. Holden's federal civil servant career began in 1983 as a Presidential Management Intern at the Naval Sea Systems Command. He holds a Ph.D. (public administration and public affairs) from Virginia Polytechnic and State University, and a Master of Public Administration (M.P.A.) and a B.A. in Public Management from the University of Maine.

DEIRDRE MULLIGAN is director of the new Samuelson Law, Technology and Public Policy Clinic at the University of California, Berkeley, School of Law (Boalt Hall). While attending Georgetown University Law Center, Mulligan worked on the American Civil Liberties Union's privacy and technology project, where she honed her interest in preserving and enhancing civil liberties and democratic values. After law school, she became a founding member of the Center for Democracy and Technology, a high-tech, civil liberties public interest organization based in Washington, D.C. For 6 years, Mulligan was staff counsel at the center. She has worked with federal lawmakers, governmental agencies, the judicial system, public interest organizations, and the high-tech business community, with the goal of enhancing individual privacy on the Internet, thwarting threats to free speech on the Internet, and limiting governmental access to private data. She has testified in several settings and contributed to technical standards development. Ms. Mulligan received her J.D., cum laude, from Georgetown University Law Center in 1994 and a B.A. in architecture and art history from Smith College in 1988.

JUDITH S. OLSON is the Richard W. Pew Chair in Human Computer Interaction at the University of Michigan. She is also a professor in the School of Information, the Business School, and the Department of Psychology. Her research interests include computer-supported cooperative work, human-computer interaction, the design of business information systems for

http://www.nap.edu/openbook/0309084008/html/44.html, copyright, 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

organizational effectiveness, and cognitive psychology. Professor Olson's recent research focuses on the nature of group work and the design and evaluation of technology to support it. This field combines cognitive and social psychology with the design of information systems. She began her career at the University of Michigan in the Department of Psychology, served as a technical supervisor for human factors in systems engineering at Bell Laboratories in New Jersey, and returned to Michigan to the Business School and the then-new School of Information. She has over 60 publications in journals and books and has served on a number of national committees, including the National Research Council Committee on Human Factors and the Council of the Association for Computing Machinery. She has recently been appointed to the CHI Academy. Dr. Olson earned a B.A. in mathematics and psychology from Northwestern University in 1965 and a Ph.D. 4 years later in the same disciplines from the University of Michigan.

JOE PATO is currently the principal scientist for the trust, security & privacy research program at HP Labs and has served as the CTO for Hewlett-Packard's Internet Security Solutions Division. Mr. Pato's current research focuses on the trust needs of collaborative enterprises on the Internet, addressing both interenterprise models and the needs of lightweight information appliances representing the interests of the individual. He is looking at critical infrastructure protection and the confluence of trust, e-services, and mobility. This work recently led him to be one of the founders of the IT-ISAC. His past work has included the design of delegation protocols for secure distributed computation; key exchange protocols; interdomain trust structures; the development of public- and secret-key-based infrastructures; and the more general development of distributed enterprise environments. Mr. Pato is currently cochair of the OASIS Security Services Technical Committee and has participated on several IEEE, ANSI, NIST, Department of Commerce standards or advisory committees.

RADIA PERLMAN is a Distinguished Engineer at Sun Microsystems Laboratories. She is the architect for a group that does research in network security issues, recently focused on PKI deployment. Some of the group's implementation will be distributed as part of a reference implementation for Java. She is the author of many papers in the field of network security, as well as coauthor of a textbook on network security and author of a textbook on lower-layer networking protocols. She is also well known for her work on sabotage-proof routing protocols. Her work on lower-layer protocols is also well known and forms the basis of modern bridging, switching, and routing protocols. This expertise is crucial to understanding the technology behind such things as providing Internet anonymity. She has about 50 issued patents, a Ph.D. in computer science from MIT, and S.B. and S.M. in mathematics from that institution. She was recently awarded an honorary doctorate from KTH, the Royal Institute of Technology, Sweden.

PRISCILLA M. REGAN is an associate professor in the Department of Public and International Affairs at George Mason University. Prior to joining that faculty in 1989, she was a senior analyst in the Congressional Office of Technology Assessment (1984-1989) and an assistant professor of Politics and Government at the University of Puget Sound (1979-1984). Since the mid-1970s, Dr. Regan's primary research interest has been the analysis of the social, policy, and legal implications of organizational use of new information and communications technologies. Dr. Regan has published over 20 articles or book chapters, as well as *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press, 1995). As a recognized researcher in this area, Dr. Regan has testified before Congress and participated in meetings held by the Department of Commerce, the Federal Trade Commission, the Social

http://www.nap.edu/openbook/0309084308/html/41.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

Security Administration, and the Census Bureau. Dr. Regan received her Ph.D. in government from Cornell University in 1981 and her B.A. from Mount Holyoke College in 1972.

JEFFREY I. SCHILLER received his S.B. in electrical engineering (1979) from the Massachusetts Institute of Technology. As MIT network manager he has managed the MIT Campus Computer Network since its inception in 1984. Prior to his work in the Network Group, he maintained MIT's Multics timesharing system during the time frame of the ARPANET TCP/IP conversion. He is an author of MIT's Kerberos Authentication system. Mr. Schiller is the Internet Engineering Steering Group's (IESG) area director for security. He is responsible for overseeing security-related working groups of the Internet Engineering Task Force (IETF). He was responsible for releasing a U.S. legal freeware version of the popular PGP encryption program. Mr. Schiller is also responsible for the development and deployment of an X.509-based public key infrastructure (PKI) at MIT. He is the technical lead for the new Higher Education Certifying Authority being operated by the Corporation for Research and Educational Networking (CREN). Mr. Schiller is also a founding member of the Steering Group of the New England Academic and Research Network (NEARnet). NEARnet, now part of Genuity Inc., is a major nationwide Internet service provider.

SOUMITRA SENGUPTA is assistant professor in the Department of Medical Informatics at Columbia University. Dr. Sengupta has focused his work on the challenges of security and privacy in health care, complementing his academic work by service as security officer for the NewYork-Presbyterian Healthcare System. His research interests are in the areas of distributed systems, their monitoring, management, and security aspects, and their application in a health care environment. He is interested in the architectural design and engineering concerns of building large, functioning systems over heterogeneous platforms and protocols. Dr. Sengupta holds a B.E. from Birla Institute of Technology and Science (Electrical and Electronics Engineering), Pilani, India, and an M.S. and Ph.D. in Computer Science from the State University of New York at Stony Brook. He was a member of the Association for Computing Machinery (ACM) from 1984 to1994, the Institute for Electrical and Electronics Engineering (Computer Society) from 1984 to1992 and is currently a member of the American Medical Informatics Association.

JAMES L. WAYMAN has been the Director of the Biometrics Test Center at San Jose State University in San Jose, California since 1995. The center is funded by the United States and other countries to develop standards and scientific test and analysis methods, and to advise on the use or nonuse of biometric identification technologies. The test center served as the U.S. National Biometrics Test Center from 1997 to 2000. Dr. Wayman received the Ph.D. degree in engineering from the University of California at Santa Barbara in 1980 and joined the faculty of the Department of Mathematics at the U.S. Naval Postgraduate School in 1981. In 1986, he became a full-time researcher for the Department of Defense in the areas of technical security and biometrics. Dr. Wayman holds three patents in speech processing and is the author of dozens of articles in books, technical journals and conference proceedings on biometrics, speech compression, acoustics and network control. He serves on the editorial boards of two journals and on several national and international biometrics standards committees. He is a senior member of the Institute of Electrical and Electronic Engineers.

DANIEL J. WEITZNER is director of the World Wide Web Consortium's Technology and Society activities. As such, he is responsible for development of technology standards that enable the web to address social, legal, and public policy concerns such as privacy, free speech,

http://www.nap.edu/openbook/0309084032/html/42.html, copyright , 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

protection of minors, authentication, intellectual property, and identification. He is also the W3C's chief liaison to public policy communities around the world and a member of the ICANN Protocol Supporting Organization Protocol Council. Mr. Weitzner holds a research appointment at MIT's Laboratory for Computer Science and teaches Internet public policy at MIT. Before joining the W3C, Mr. Weitzner was co-founder and deputy director of the Center for Democracy and Technology, an Internet civil liberties organization in Washington, D.C. He was also deputy policy director of the Electronic Frontier Foundation. As a leading figure in the Internet public policy community, he was the first to advocate user control technologies such as content filtering and rating to protect children and avoid government censorship of the Internet. These arguments played a critical role in the 1997 U.S. Supreme Court case, *Reno v. ACLU*, awarding the highest free speech protections to the Internet. He successfully advocated for adoption of amendments to the Electronic Communications Privacy Act creating new privacy protections for online transactional information such as Web site access logs. Mr. Weitzner has a degree in law from Buffalo Law School and a B.A. in philosophy from Swarthmore College. His publications on communications policy have appeared in the *Yale Law Review*, *Global Networks*, *Computerworld*, *Wired Magazine*, *Social Research*, *Electronic Networking: Research, Applications & Policy*, and *The Whole Earth Review*. He is also a commentator for NPR's Marketplace Radio.

STAFF:

LYNETTE I. MILLETT is a study director and program officer with the Computer Science and Telecommunications Board of the National Research Council. She is currently involved in several CSTB projects along with the authentication study, including a comprehensive exploration of privacy in the information age and a study examining the fundamentals of computer science. She is also exploring possible study options for CSTB with respect to the issues of open source software development, dependability of complex software systems, and women in computer science. She recently completed the CSTB study that produced *Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers*. Before joining CSTB, she was involved in research on static analysis techniques for concurrent programming languages as well as research on value-sensitive design and informed consent online. She has an M.Sc. in computer science from Cornell University. Her undergraduate degree is in mathematics and computer Science from Colby College. Her graduate work was supported by both an NSF graduate fellowship and an Intel graduate fellowship. While at Cornell, Millett cofounded its Engineering Graduate Student Association.

JENNIFER BISHOP is a senior project assistant with the Computer Science and Telecommunications Board of the National Research Council. Before moving to Washington, Ms. Bishop worked for the City of Ithaca, New York, coordinating the Police Department's transition to a new SQL-based time accrual and scheduling application. Her other work experience includes designing customized hospitality industry performance reports for Ithaca-based RealTime Hotel Reports, LLC., maintaining the police records database for the City of Ithaca, and hand-painting furniture for Mackenzie-Childs, Ltd., of Aurora, New York. She is an artist working in oil and mixed media and is currently attempting to make her professional debut in the Washington art scene. Ms. Bishop holds a B.F.A (2001) in studio art from Cornell University.

http://www.nap.edu/openbook/0309084303/html/43.html, copyright 2001 The National Academy of Sciences, all rights reserved

PREPUBLICATION VERSION
SUBJECT TO FURTHER EDITORIAL CORRECTION

Appendix B

What Is CSTB?

As a part of the National Research Council, the Computer Science and Telecommunications Board (CSTB) was established in 1986 to provide independent advice to the federal government on technical and public policy issues relating to computing and communications. Composed of leaders from industry and academia, CSTB conducts studies of critical national issues and makes recommendations to government, industry, and academic researchers. CSTB also provides a neutral meeting ground for consideration of complex issues where resolution and action may be premature. It convenes invitational discussions that bring together principals from the public and private sectors, assuring consideration of all perspectives. The majority of CSTB's work is requested by federal agencies and Congress, consistent with its National Academies context.

A pioneer in framing and analyzing Internet policy issues, CSTB is unique in its comprehensive scope and effective, interdisciplinary appraisal of technical, economic, social, and policy issues. Beginning with early work in computer and communications security, cyber-assurance and information systems trustworthiness have been a cross-cutting theme in CSTB's work. CSTB has produced several reports known as classics in the field, and it continues to address these topics as they grow in importance.

To do its work, CSTB draws on some of the best minds in the country, inviting experts to participate in its projects as a public service. Studies are conducted by balanced committees without direct financial interests in the topics they are addressing. Those committees meet, confer electronically, and build analyses through their deliberations. Additional expertise from around the country is tapped in a rigorous process of review and critique, further enhancing the quality of CSTB reports. By engaging groups of principals, CSTB gets the facts and insights critical to assessing key issues.

The mission of CSTB is to

- ***Respond to requests*** from the government, nonprofit organizations, and private industry for advice on computer and telecommunications issues and from the government for advice on computer and telecommunications systems planning, utilization and modernization;
- ***Monitor and promote the health of the fields*** of computer science and telecommunications, with attention to issues of human resources, information infrastructure, and societal impacts;
- ***Initiate and conduct studies*** involving computer science, technology, and telecommunications as critical resources; and
- ***Foster interaction*** among the disciplines underlying computing and telecommunications technologies and other fields, at large and within the National Academies.

As of March 2002, CSTB activities with security and privacy components address privacy in the information age, critical information infrastructure protection, authentication technologies and their privacy implications, information technology for countering terrorism, and geospatial information systems. Additional studies examine broadband, digital government, the

http://www.nap.edu/openbook/0309064300/html/44.html, copyright , 2001 The National Academy of Sciences, all rights reserved

fundamentals of computer science, limiting children's access to pornography on the Internet, digital archiving and preservation, and Internet navigation and the domain name system. Explorations touching on security and privacy are under way in the areas of the insider threat, cybersecurity research, cybersecurity principles and practices, dependable/safe software systems, wireless communications and spectrum management, open source software, digital democracy, the "digital divide," manageable systems, information technology and journalism, supercomputing, and information technology and education.

More information about CSTB can be obtained from <http://www.cstb.org>.