HEARING OF THE GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS SUBCOMMITTEE OF THE HOUSE GOVERNMENT REFORM COMMITTEE

-

SUBJECT: DOES AMERICA NEED A NATIONAL IDENTIFIER?

-

CHAIRED BY: REPRESENTATIVE STEPHEN HORN (R-CA):

-

WITNESSES PANEL I:

-

HONORABLE NEWT GINGRICH, FORMER SPEAKER OF THE HOUSE OF REPRESENTATIVES;

-

HONORABLE ALAN SIMPSON, FORMER MAJORITY WHIP OF THE SENATE;

-

HONORABLE BILL MCCOLLUM, FORMER CHAIRMAN, HOUSE OF REPRESENTATIVES PERMANENT SELECT COMMITTEE ON INTELLIGENCE, SUBCOMMITTEE ON HUMAN INTELLIGENCE, ANALYSIS AND COUNTERINTELLIGENCE AND FORMER CHAIRMAN, HOUSE OF REPRESENTATIVES JUDICIARY COMMITTEE, SUBCOMMITTEE ON CRIME;

-

PANEL II:

-

JONATHAN TURLEY, SHAPIRO PROFESSOR PUBLIC INTEREST LAW, GEORGE WASHINGTON UNIVERSITY LAW SCHOOL;

-

HONORABLE ROY M. GOODMAN, CHAIRMAN, INVESTIGATIONS COMMITTEE, NEW YORK STATE SENATE;

-

KATIE CORRIGAN, LEGISLATIVE COUNSEL ON PRIVACY, AMERICAN CIVIL LIBERTIES UNION;

-

RUDI VEESTRAETEN, COUNSELOR AND CONSUL, EMBASSY OF BELGIUM;

-

TIM HOECHST, SENIOR VICE PRESIDENT OF TECHNOLOGY, ORACLE CORPORATION;

-

BEN SHNEIDERMAN, PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF MARYLAND, FELLOW, ASSOCIATION FOR COMPUTING MACHINERY

LOCATION: 2154 RAYBURN HOUSE OFFICE BUILDING, WASHINGTON, D.C.

Federal News Service

November 16, 2001, Friday

Section: Washington-dateline general news.

Length: 30757 words

Body

REP. STEPHEN HORN (R-CA): The quorum being present, the hearing of the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations will come to order.

Only two months after the devastating terrorist attacks of September 11th, this nation is just beginning to understand the dimensions of a dramatically ***changing*** world. Preserving the American way of ***life*** requires adaptation and sacrifice. It means using this nation's unique strengths to address the vulnerabilities that terrorists exploited at an enormous human toll. Technology is one of America's greatest strengths. In recent weeks some have called for using that technology to combat terrorism by developing a national identification system. Proponents of such a system argue that a hi- tech national identifier system linking federal and state databases would allow authorities to spot terrorists before they attack.

Some of the September 11th terrorists were in the United States illegally. Supporters say that had such a system been in place, airline personnel would have been able to crosscheck passenger lists against various watch lists. The airlines would have known that the men should not have been in the country, let alone on an airplane. Those who oppose such a system are concerned about the impact a national identifier system would have been on the very precepts of America's freedoms.

Given the vast amount of personal information that could be placed in a national identification system, there is legitimate cause for concern over its potential abuse or mismanagement. In the event that such a system were adopted, it must incorporate sufficient safeguards to prevent the abuse of power by those who would have access to the information and those with the authority to demand an individual's identification.

The technical issues involved in a database project of this magnitude must also be considered. Is it possible to develop a system that is both fraud resistant and secure? Freedom is the most precious gift to Americans. The terrorists knew it and took good advantage of it. Freedom itself was the target of the September 11th attacks. If that freedom is lost in the pursuit of justice, the terrorists will have won, even if they themselves are punished. Although holding firm to America's freedoms, we must also be open to new ideas. The survival of this great nation may depend on it.

I welcome our witnesses today and I look forward to their testimony. But before giving you the oath I will yield time for the ranking member, the gentlewoman from Illinois, Ms. Schakowsky, and -- for an opening statement.

REP. JANICE D. SCHAKOWSKY (D-IL): Thank you, Mr. Chairman, and I want to thank this panel of witnesses for coming here today.

In the wake up September 11th we're faced with an enormous challenge of balancing the need for enhanced national security with the need for protecting civil rights of the public. In the past, some efforts in the name of

national security, in my view, have ***gone*** too far and have endangered those liberties. We've learned that once that kind of harm is done, it's difficult to repair.

During World War 2 we uprooted thousands of Japanese Americans and placed them in internment camps. It is generally recognized today, over 50 years later, that the internment was a mistake. In fact, it was clear at the time that there was no danger of sabotage from those individuals. As historian Margo Anderson points out, in November 1941, in response to a request by President Roosevelt, John Franklin Carter wrote to the president, "There is no Japanese problem on the coast. There will be no armed uprising of Japanese." Nonetheless thousands of Japanese Americans, many of whom were citizens, were rounded up and placed into camps.

Today we have a monument to those that were mistreated just north of the Senate office buildings, and our government has officially apologized. However, getting to that apology and the monument was extremely difficult and did not repair the harm done. Liberty and sense of security lost by those interns cannot be given back. We must be careful not to repeat the mistakes of the past.

Last week on Thursday, before Veteran's Day, I ***went*** to the floor of the House to pay tribute to those who have served our country in the defense of freedom. We have fought hard throughout our history to maintain a free and open society. We must not sacrifice those freedoms in the name of war. If we sacrifice our freedom, we lose the war no matter what the military outcome.

The security measures we proposed in response to terrorism must pass three tests. Are they effective? Can they be applied without discrimination? Can they be implemented without sacrificing our fundamental freedom of due process, privacy and equality? The proposal for a national identification system is not new. It has failed in the past because it cannot pass these fundamental tests. The Congress passed an Immigration Reform Act in 1996, which contained a number of provisions that would have led to a national identification system. Since that law was passed, those provisions have steadily been tiered back. One provision was repealed and another modified to the point where it could not be administered at the land border between the United States and its neighbors.

In the Patriot Act, the House has reaffirmed those provisions knowing that they had no teeth. The events of September 11th show us that systems like national identification cards will not deter crazed terrorists from their mission. Those terrorists all have driver's licenses, credit cards and Internet accounts. I urge all of us and each of you to pay close attention to the effects your proposal will have on the fundamental freedoms on which this country was founded: freedom of speech and religion, freedom to assembly, freedom of the press, freedom from unreasonable search and seizure, and freedom from imprisonment without due process. Those freedoms cannot be ignored in the name of homeland security. As members of Congress we must evaluate any proposal offered in the name of enhanced security. Does it do what it claims to do? What is the burden on the public in terms of time consumed and freedom lost? Do the benefits outweigh the cost? Is there an incremental gain in security and does it justify the loss of freedom?

I look forward to hearing the testimony today and hope our witnesses will help us answer these important questions. And I thank you, Mr. Chairman.

REP. HORN: I thank you and before I call on Ms. Maloney, we have two members of the committee which will be before us, and without objection we'll have Mr. Castle and Mr. Miller.

Mr. Castle.

REP. MICHAEL N. CASTLE (R-DE): Well, thank you very much, Mr. Chairman. I know I'm an interloper here today and I appreciate you and the ranking member allowing me to appear. And I wanted to share some thoughts I have on this and some legislation I've been working on with Congressman Jeff Flake of Arizona with respect to this issue. But I must comment first that this is a very distinguished but even more so very interesting panel. I look forward to what they have to say.

Many of the issues that are involved in the subject matter of today of national identification cards in my judgment should first be addressed in managing foreign visa holders in the United States of America. While I understand that the issue of national ID cards is extremely important in the times we are ***living*** in, and I would imagine somewhat controversial if I had to place a wager on it, I believe that we must first begin with the tracking of foreign guests in our country and I don't think this should be controversial.

I would like to just share a few statistics with you. In 1998 the Immigration and Naturalization Service, INS, reported that 30.1 million foreign people came to the United States on a temporary basis. Of this 30.1 million, there are an estimated five to eight million illegal immigrants ***living*** in the United States; 40 percent of which were listed as overstays by the INS. That means they stayed beyond the time of their visa. I believe very strongly, and Mr. Flake does as well, that we need to be able to monitor all foreign visitors and track in real time -- that is, the actual knowledge on a computer screen in real time -- who they are, what their background is and what they are doing in our country.

Congress has actually -- probably in the time of the gentlemen who are on this panel -- has actually taken steps on this, but none of this has really been implemented. Six years ago Congress instructed the INS to gather the arrival and departure date of most foreign visitors, to make sure they do not remain in the United States after the expiration of their authorized stay. However, to this day the INS Passenger Accelerated Service System, INSPASS is its acronym, remains only a pilot project used at only four airports, but not at any land or sea port points of entry.

Another example of an innovative idea which has been put in place but not fully used, is the border crossing card which is used by ***Mexican*** and Canadian nationals who seek admission as border crossers. But, again, this program has been plagued by difficulties and delays. I think such examples illustrate the lost opportunities inherent in the poor management of tracking systems.

To address immigration challenges, Representative Flake and Representative Deal of Georgia and I did introduce an act called the Visa Integrity and Security Act to strengthen the immigration system and to ***improve*** the ability of the INS to track all these temporary visa holders. A number of the key provisions in this legislation were actually included in the Patriot Act, which you might know as the Anti-Terrorism Act, which passed very recently in the Congress of the United States.

But there is still a lot of work to be done. We do need to be able to track and locate temporary foreign visitors to the U.S. to ensure they are here for their stated purpose, which could be anything from being a student, to working, to a visitor, and to know when they have come and when they have left.

A student tracking system that's been under development since 1997 needs to be ***improved*** and fully implemented. The Patriot Act does call for the implementation of the Student Tracking System and has authorized $36 million, which is a good start towards its deployment. However, we must advocate that the INS incorporate key provisions in any future student tracking system. We need to know if foreign students actually enroll in classes and whether they drop out. There are over 500,000 foreign students in the United States now. We also need to know their family history, course of study and date of enrolment.

Second, we need to know if a temporary ***worker*** holding an H1B visa, which has been the subject matter of many an hour here in the Congress, is still working at the company that hired that person. A crucial aspect of any effective system that tracks foreign visitors is the use of technology to foil would be counterfeiters, of which there are many, I might add.

A Smartcard visa for foreign visitors would be much more difficult to forge than traditional visas. It would hold a copy of the fingerprint biometric and typical visa information; or pupil of the eye or whatever biometric one would want to use. This is not a new idea either, by the way. It just has not been implemented particularly well. U.S. citizens across the border frequently are able to participate in a voluntary program that registers the fingerprint biometric. We just think in certain instances it should be automatic that it be done, as opposed to being a voluntary program.

Holders of frequent traveler passports pass more quickly through Customs by showing their fingers for identification at a Customs station. The use of biometric technology is encouraged in the Patriot Act. These tamper-resistant visas could eventually be linked to an integrated computerized entry access system and the INS, Customs, consulates, universities and other law enforcement agencies would all work off the same information to monitor and track students, tourists and other visa holders. And I'm sure I'm not telling anybody here the difficulty of some of the information exchange, even among governmental agencies today, much less on a computer in real time in terms of the various places, the embassies, the points of entry where that information would be usable.

All this technology is available, by the way, although at a cost. And programs could be more effectively utilized to track our foreign guests. The lessons learned from tracking foreign visitors can lend important insight to the pros and cons of enacting a national identification card for United States citizens, which we may or may not be ready for now. But I think we are ready for a visa system at this point, if we put our minds to it and ***go*** about it.

Let me just say in conclusion, in no way am I advocating limiting in this particular program what we are doing with respect to visas or visitors to our country. We just want to make sure we know who's coming into this country and, if they should not be coming into this country, are preventing them from being here and while they are here, they are doing what they are supposed to be doing. And I appreciate the time, Mr. Chairman. Again, I realize I'm an interloper and you've been very generous and I yield back the balance of my time.

REP. HORN: Thank you very much and now I yield to the ranking member over the years and the gentle lady of New York, Ms. Maloney.

REP. CAROLYN B. MALONEY (D-NY): Thank you and I would first like to thank you, Mr. Chairman, and the ranking member for holding this hearing and commend you for tackling yet another complicated and controversial issue. Also, I'd like to extend my appreciation to the very interesting panelists we've assembled here today for taking the time to be here.

We have taken a hard look at the way our great nation operates since September 11th. The hard, cold truth is that we have been very lax in many areas of safety and security.

I believe the most difficult fact for us as a nation to face is that there is a group of individuals who hate us and want to do harm to the citizens of America. As an elected official, I must do everything that I can to protect my constituents and the constituents of our country. In this new world, I am not exactly how sure we can accomplish this. However, I'm eager to learn and understand more, as we will learn today.

In the month of October alone we had 17 million people travel across the borders of the United States. We welcome all travelers. Our nation's economy depends in part on these visitors. However, we have to face this cold, hard truth that not everyone entering our borders enters with good intentions. Access to the United States must be looked upon as a privilege, not a right. Our country's founders provided many safeguards to protect our freedom while ensuring our safety.

One of the duties of our democracy is that it is not static, but a robust ***living*** thing that can ***change***, and times have dramatically ***changed***. Daniel Webster, one of our nation's former great leaders, once stated, "God grants liberty only to those who love it and are always ready to guard and to defend." Today, we must guard and defend it. We must not be afraid of new ideas. We need to protect not only the rights of individuals, but their ***life***.

We pride ourselves of the many freedoms we have in the United States. However, in order to protect these freedoms we need to protect our safety and our nation's security. I commend President Bush for taking the bold step yesterday to begin to acquire stricter regulation regarding the granting of visas. Fear has struck the core of the community I represent in New York -- I lost well over 600 constituents -- and it has struck the core of the American people.

The freedom to travel freely about our nation has taken a devastating blow. We now have armed guards on several flights, with the implementation of complete coverage for all flights ongoing. We look to our law enforcement to protect and to serve. However, we need to arm them with the tools to accomplish this mission. A more thorough and smarter Green Card for non-U.S. persons, I believe, is a beginning. I also believe that we need to tie one's state driver's license to their visa expiration date.

During a hearing held in New York on terrorism, Governor Jeb Bush provided testimony that in his state of Florida one's driver's license expires on the same date as their visa. Does this not provide yet another way of tracking non-U.S. persons? I believe we need to take other steps and one could be that an individual's bank account could be frozen at the time of the visa expiration date. All non-reclaimed funds could revert to the state's escrow account to fight terrorism. We have seen how our banking industry has been contaminated by the terrorist community again, and we need to reclaim it. As I stated earlier, I do not have all the answers so I'm very much looking forward to our panelists to help me and other members of this committee uncover all the pros and cons of this important issue.

Thank you very much and I yield back, Mr. Chairman.

REP. HORN: Thank you, and we now yield to Mr. Miller from Florida, the chairman of the Census Subcommittee of Government Reform.

Mr. Miller.

REP. DAN MILLER (R-FL): Thank you, Mr. Chairman. Thank you for calling this hearing. I'm delighted with the two panels and I'll be very brief because I heard the speaker talk about this issue briefly at a breakfast about two weeks ago. And ever since September 11th it's raised a lot of issues of which direction to ***go*** -- civil liberties issues and I know this will be addressed by the panel, the privacy issue which I know Mr. McCollum has worked on a lot. Technology, which is something the speaker talks about all the time. And just to make sure our country can function after -- post September 11th, our economy can function.

So there's a lot of challenges and interesting comments, and I'm really here to listen and learn, so I yield back.

REP. HORN: Thank you very much, and any other statements that come in will be filed for the record.

We now start with our first panel, and I think you know the routine that this is an investigating committee, and so if you raise your right hand and if you have any assistants backing you up, get them and the clerk will get their names too.

Do you solemnly swear the testimony you will give before this subcommittee will be truth, the whole truth and nothing but the truth?

WITNESSES: I do.

REP. HORN: The clerk will note that all the witnesses have affirmed, and we start with the Honorable Newt Gingrich, former speaker of the United States House of Representatives.

Mr. Speaker.

MR. NEWT GINGRICH: Thank you very much, Mr. Chairman, and I want to thank you and the ranking member for holding this hearing. I also wanted to take this opportunity to commend you for your consistent leadership on the issue of cyber security and fact that this subcommittee has been very far ahead of events in looking at the need for effective technology in the security area.

I also want to begin with Mrs. Schakowsky's I think absolutely correct point, which is that we have to design -- the challenge to the Congress and the president is to design a system which both provides civil liberties protection for the innocent and protection of the innocent. In the past with things like fingerprinting, wire tapping and other

technologies, we worked very hard to make sure that while we were strengthening law enforcement, we were never infringing on the innocent, and I think this has to be thought through in a very careful way.

The fact is we already have a primitive, inefficient, easily cheated system of identification. I flew out of Reagan National yesterday and three times I produced an ID card. Now, I just want to point out every audience I talk to around the country, I ask them how many of them know someone who in high school had access to an ID card that might not have been their own, for reasons we won't ***go*** into. And, while no one personally had ever used an ID card for an inappropriate purpose, it has always amazed me the number of people who seemed to find at 16 or 17 access to an ID card.

So I want to be very clear. I think we've already indicated at airports, we've indicated at government buildings, we've indicated in a variety of places that asking for identification is legitimate. The question now is can we design a system which has effective ID, while still protecting the innocent? I think that it has to be an American model of security which means a high technology, capital intensive system that provides security, speed, efficiency and convenience. That's the model we've always set for ourselves and I think, frankly, the current lines at airports are a sign we don't have a system that meets that test.

It's also necessary for the world economy to have a parallel system for freight, whether it's in trucks or container cargo, that is secure, fast and efficient or we will literally break down the world economy and add a substantial amount of cost to everybody's ***life***.

I would suggest to this subcommittee that as you look at these, that you look very seriously at outsourcing as much production as possible, because most of the great breakthroughs that are high technology and capital intensive occur in the private sector, and occur in entrepreneurial businesses. And I particularly would recommend to you Clayton Christensen's "The Innovators Dilemma" as a study of new technologies at work and Nathan Mirbald's (ph) recent writing, particularly in USA Today, on the concept of exponential industries and the ability to develop really dramatically new technologies in the next five to ten years.

I personally think we're ***going*** to want to end up with a biometric solution that involves either a retinal or iris scan, which I think is harder to cheat than a thumbprint and, frankly, is as easy to measure in real time; it's simply a picture. And any of us who are being filmed for television or by still photographers are having exactly the same experience you'd have for a retinal scan.

I want to distinguish also civil liberties for American citizens from foreign visitors. I believe that all foreign visitors should be scanned as they enter the country.

We ought to have a databank either of their iris or retina; I think that's a technical decision which one you're using. But we ought to be able to know who you are. We ought to be able to match you up against a system that would indicate whether you were a known drug dealer, a known terrorist, et cetera. And it would basically indicate and attach to an identity that had a biometric on the identity card, so we knew that the person we're talking to didn't just buy this for $11 in Los Angeles on a street corner, as can currently be done.

For Americans, I think it's fairly simple to have the 50 states ***go*** to a biometric measure on the driver's license and simply ensure that all of the states -- 50 states plus D.C. that the databases are linked. That means an investment in wireless, high speed connectivity with very high speed computing. But, literally, it's no harder for a policeman standing and talking to you by the side of your car within seconds to have verified who you really are, if we design a system that does it. And I think you can do that with civil liberties protected.

I would not insist on a national ID card, because I think you do get into civil libertarian issues. But I would suggest to you that the simple act of having two lines at airports, one biometric where anybody who's a frequent flyer who wanted to be able to literally walk through the line, verify who they are and pick up their ticket at security as they're ***going*** through. While we'd have a long line that may take an hour and a half for people who prefer to avoid that

kind of convenience. I think you'd find a natural migration of over 90 percent of the American travelers, within a year or less, to the higher speed line.

Let me also suggest that the committee look at the emerging technology at MIT and elsewhere, that for somewhere between one and 30 cents per suitcase you could literally have an embedded wireless system that would enable you to track literally every suitcase. And if you introduced it as a manufacturing process now, you would within five or six years have an overwhelming tagged and identified, highly secure system.

As I said earlier, this kind of thinking I think has to also apply to trucks and the container cargoes. And if you look at what UPS and FedEx already do, you can see the beginnings of a model that, given the high -- the new breakthroughs and the technologies, could be even more sophisticated and even more accurate.

Let me just close by ***going*** back to the exactly correct warning that Mrs. Schakowsky made. There is no question in my mind that we can design, just as with medical records, an ability to have personal privacy and access to information that may save our ***lives***. But that requires a federal law that makes it a felony to use that medical record inappropriately.

Similarly, I think you can design a system which allows you to track a person who is genuinely out to do something bad, without in that process either dramatically inconveniencing or harming those who are innocent. And, in fact, I would argue that if the American people knew that every employee who walked on an airport had some means of checking to make they were really the person they claimed to be, if we knew that our FBI, CIA, FAA computers worked, the notion -- I just want to close on this notion, because what you're doing on this subcommittee is so vital.

Six weeks before September 11, the Central Intelligence Agency told the Federal Bureau of Investigation two terrorists had entered the United States. Six weeks later they had still not been able to get that information into the airline computers, and two of the terrorists on September 11 in Boston boarded the airplane under their own names, 42 days after the United States government officially knew they were in the U.S. and they were very dangerous.

Now, I simply suggest ***going*** to a mandatory, regular ID card won't help much, because with desktop printing they will learn how to buy cards that are false. But if we had a high speed computing system and we had an ability to have very high speed access, I think we could design a system where we would have found those two people, they would have been stopped at Logan and we would have had a very significant understanding of what was ***going*** on.

I think this committee is moving in the right direction. If it does it right, the system will be very secure, it will be very safe, and it will protect our civil liberties while also protecting us.

REP. HORN: We thank you very much for those pertinent views, which I'm used to, and it's very useful. We now turn to the very distinguished ex-senator and one of the great public servants of this country, namely Alan Simpson, who has spent more time on immigration I think than probably all the rest of us put together. So I'm ***going*** to turn it over to you.

REP. SCHAKOWSKY: Mr. Chairman, if I could just inquire. Apparently you're ***going*** to proceed through the vote?

REP. HORN: No, we're ***going*** to ***go*** now and when Mr. Miller returns, he will be presiding, and then I'll come back. We're in this less than seamless operation --

MR. : We know that.

REP. HORN: -- known as the vote. And we'll be back, so --

MR. ALAN SIMPSON: I'll just proceed then. Thank you.

REP. HORN: Proceed and I will try to be back in six or seven minutes.

MR. SIMPSON: Thank you, Chairman Horn.

REP. HORN: Thank you.

MR. SIMPSON: I come in here with a very eerie feeling as Jack Brooks is staring at me there. He would look at me with that smoldering cigar and say, "Simpson, I got a deal for you."

(Laughter.)

I'd lose my shirt and my underwear and everything else in here. Well, that was Jack Brooks. What an amazing man.

It is a pleasure to be here to discuss this serious issue of how we might strengthen domestic security. I was particularly moved by Congresswoman Schakowsky's remarks, for I met Norm Mineta at the Heart Mountain Relocation Center when we were 12-year-old-boys. He was behind wire and I were ***living*** in Cody, and our scout master took us to the Jap camp -- that's what it was called. Eleven thousand people there, and Norm and I struck up a friendship of curiosity and juvenile devilment that has lasted now 70 years. He's a very dear and special friend.

But we want to remember at that time that Attorney General Warren, Earl Warren of California, signed the order to evacuate them and the unanimous decision of the United States Supreme Court by William O. Douglas said that it was proper. So I think let's try to keep that in perspective and not think of how it is 50 years from then as to the fact that the Japanese submarine lobbed a couple of shells into an oilfield off of California in the spring of '42, and it kind of startled people. Just thought I'd pitch that in. Just thought I'd throw it in there.

Anyway, you're on track. I was impressed by what Newt is saying because you're all being led astray by a single term, and the term is national ID. I never used it. I put it in the bill that we were not talking about a national ID and you'd do a disservice to the country when you use the phrase national ID. We're talking about a more secure identifier system. It could be many things. And if anyone believes that there is intrusiveness in what we're suggesting, all of us -- Newt, myself, what Bill will say, what Democrats and Republic -- what Rodino and I said, what Mazzoli and I said. And in the bill it said we're not talking about a national ID. That's a diversion for people who like to talk about tattoos and Nazi Germany, and don't let them get away with it.

We're not talking about that. Every time we try to do something in this area it was filled with emotion, fear, guilt, and racism. The Select Commission on Immigration Refugee Policy said we ought to do something in this area. We tried to do that, got shot out of the saddle by arguments about tattoos and Nazi Germany. Then we tried it again and we had a biometric activity in one of them, and in a conference committee in the middle of the night when on the floor of the House, passed the Senate, there was a highly emotional argument about, again, Nazi Germany and tattoos. It was pulled out and dear old Joe Moakley took it out and we passed it in the middle of the night without anything in it.

The House always had an aversion to that kind of thing.

The Senate would pass it and I can only share with you that everything we did in this area was bipartisan. Mazzoli, our Democrat from Kentucky; Rodino, the chairman of the Judiciary Committee from New Jersey -- still ***living*** and a magnificent man -- we did these things. Hamm Fisch (ph) -- and Newt knows him well and so does Bill. You have to do something and the something is not intrusive any more than what you get when you ***go*** to the airport now, or what you get when you ***go*** into a store and have to give your slide card, or when you file for credit or whatever it may be.

REP. SCHAKOWSKY: Senator Simpson.

MR. SIMPSON: Yes, indeed?

REP. SCHAKOWSKY: I'm afraid I have to ***go*** vote, which would leave no members here and so I'm ***going*** to grab this gavel while I can --

MR. SIMPSON: (Inaudible.)

REP. SCHAKOWSKY: -- and recess this committee at least until someone returns. All right.

MR. SIMPSON: Well, that's very kind, thank you. I'll just keep ***going*** though. No.

(Laughter.)

(Recess)

REP. MILLER: The subcommittee will come back to order. Mr. Horn will be back shortly and he asked me to proceed with the presentation.

Senator Simpson, would you continue?

MR. SIMPSON: Thank you very much, Congressman Miller, and I see you have new devices here which are very clever. It's not on yet, so I'll -- it is?

Well, I was just kind of reviewing things and speaking to Congresswoman Schakowsky's comments. Let me just give you a very brief summary of past efforts. The select commission came into being '79 to '81. I was a member of that bipartisan commission, Father Ted Hesburgh was chairman, and we did a lot of things. We recognized that no system attempting to control anything would be effective without a more secure method of confirming a person's identity and immigration status.

So we recommended -- the commission recommended it. It was a narrow vote, a substantial improvement. Then we had Immigration Reform and Control Act of '86. When that first passed, it had a provision in it that the executive branch would implement a system that would reliably determine identity, again, and authorization of all persons. That was weakened by the Senate, stripped by the House. I think it was a conference committee, and that's often the history of conference committees as I recall them here in this chamber, especially with Brooks with the gavel. But anyway, that's an aside.

The enacted version of IRCA had a pilot program in it and then we had telephone verification. We couldn't get much done because, again, the background noise was always national ID. The initial conference committee version of the Immigration Act of '90, where we broadened legal immigration a great deal, contained a pilot program using biometric data to make state drivers' licenses more secure. And it was then, to the amazement of Democrats and Republicans alike, that that issue was demagogued in the most grotesque way one evening in this body, and the House rule was defeated. And Joe Moakley brought it back from the dead and we got it out, but it was stripped again.

Then Barbara Jordan came to the floor, a most amazing woman, and she did the Jordan Immigration Commission on Immigration Reform. She recognized it was too susceptible -- the present system was too susceptible to discrimination against foreign-looking and foreign-born or foreign-sounding ***workers***. So she commended a computerized registry using data provided by Social Security and the INS, and suggested pilot programs for employers to use these databases to be conducted in states with the highest immigration rates.

Then along came the '96 bill. I had little to do with that because we did nothing to do anything to curb illegal immigration -- or legal immigration, rather, as Barbara Jordan recommended. But we did get a pilot program in there to -- where you could access via computer modem. In '97 it was used by approximately 2,000 employers, who were voluntarily using it. While it's a helpful deterrent to certain instances of fraud, it is not a good one. An unauthorized alien submits a card with an invalid number or submits a card where the name does not match the number. It does not prevent aliens who falsely assume the identity of another person from using the other person's valid Social Security number, and this is often referred to as identity theft or true identity fraud, and it is endemic in America. Talk to your credit card people.

So I doubt that there is any full support for a national ID card. I never suggested it and I just have to pack that in one more time. And if that's ***going*** to be the word, you're ***going*** to all fail. You will do nothing. Get away from it. It's a phoney baloney. What we're talking about is -- and when we were talking about it then, was some type of new document to establish work authorization or identity. We were talking about perhaps a card that would not be carried on your person, not be used for law enforcement, have the maiden name of your mother on the back of it and the birth date. And then, you know, always would come the George Orwellian aspects of that.

Here's what I suggest, respectfully. A few positive benefits, I think. I therefore would respectfully suggest that you ***improve*** the state drivers' licenses. That's the principal identity document in our country. We must eliminate the ability of people to falsely assume the identity of another. Some of the September 11 terrorists facilitated their actions through easy access to Virginia drivers' licenses. Now, the only way to prevent identity fraud is to include biometric data on the card, I agree with Newt completely, such as a fingerprint. It is also -- in California it is done with a retina scan in California for commercial drivers' licenses, and you ought to take a look at that. Minimum nationwide issuance standards could be imposed by Congress or agreed upon by the states. I think it would be minimally intrusive.

Expanded access, would be another one, to INS and Social Security databases. Extend the basic pilot program not just California, New York, Texas, Florida, Illinois. Include other states, have access to that base. But, of course, that would require more funding for the Social Security Administration and directing to ***improve*** the accuracy of the database, and here's the one that everybody misses. There are about 2,000 agencies in the United States that issue a birth certificate. They love it. They're little old ladies, they do things -- little old men too, and they issue them and they love it and they don't want anybody to mess with it. Don't mess with me giving -- because I know the mother and the father and when little twinkletoes was born, I signed that.

The vulnerability of the birth certificate system allows aliens to bypass all immigration systems altogether and impersonate U.S. citizens. The Jordan Commission said if we reduce the fraudulent access to the breeder documents, start looking at the breeder documents, ladies and gentlemen of the Congress; particularly birth certificates that can be used to establish an identity in this country.

And the specific steps recommended by her commission were, and I conclude, regulation of requests for birth certificates through standardized application forms. A system of interstate and intrastate matching of birth and death. We don't do that in America; we don't match birth and death. How can you ever get a handle on it? Requiring a federal agency only accept certified copies of birth certificates and a standard design and paper stock for all certified copies, and encourage states to computerize birth records repositories. I think these recommendations are sensible, practical and should be enacted and it is time. Thank you very much.

REP. HORN: Thank you, Senator. As usual, you have the common people's touch and you also know how to get through the bureaucracy and everything else. I am glad to say to you the commissioner yesterday told a number of us that he will split up the agency, so that you've got an enforcement operation and you've got a service operation. And a lot of us have wanted that over the years, so a little progress is being made there.

We now ***go*** to Mr. McCollum, who, during my years in the House, no one was a better legislator than he was. And we're glad to have you back here, Mr. McCollum.

MR. BILL MCCOLLUM: Well, that's a high compliment, Mr. Chairman, and I'm very glad to be back here too today with you and especially pleased to be with this distinguished panel of my friends, Speaker Gingrich and Senator Simpson, with whom I've served a good number of years, and on a topic that really is very timely and very important.

I know, like everybody here, that we all were affected terribly by this tragedy on September 11th, the attacks on us that I think most envisioned was unimaginable. Even though many of us who served in the arenas that I did in Congress knew that sooner or later we were ***going*** to have a terrorist attack of some magnitude, we could not have expected nor anticipated the horror that came with this particular one. And now we're having a reaction to that.

Having been chairman of the Crime Subcommittee, having chaired the Subcommittee on Human Intelligence, founded the Terrorism Task Force, spent 18 of the 20 years served on Immigration Subcommittee, many of those years with Senator Simpson's work and mine together, with the fellow up there you mentioned, Brooks, and others, I come to this with a perspective of absolute conviction about a couple of things.

One of those is that there is no need for a national identification card, and I am very much opposed to one. But I think it's important to identify what a national identification card is. What do we mean by that? Mr. Chairman, I mean by that a uniform system -- a uniform card that every American would be required to carry to produce to law enforcement, employers, various government agencies for identification purposes. Such a card would contemplate a national database, access by computer for verification purposes. It might contain a strip on the back like your Visa Card does. It has data and information already built in it, or accessible through computer, a photograph of fingerprint, possibly even a national database that every American had a fingerprint in. I don't favor that, I don't think that's right, I think that's an insult to our system of government, the privacies and those great freedoms that our founding fathers envisioned. The Big Brother type system.

But we do need to make some of the identifiers we already have work, and that's what all of us are testifying about today. I have not heard a word that either of my colleagues said that I took umbrage with, but I do have a perspective on a couple of these, a little bit differently.

First of all, I believe that the Social Security card desperately needs to be made more secure. There's been great resistance to doing much with that card over the years, but back in 1996 -- excuse me, 1986 when the Simpson-Mazzoli bill passed, and then more in the amendments of 1996 in the immigration world for employer sanctions and when you ***go*** to get a job, the two principal identifiers became narrowed down to your driver's license and your Social Security card. So if you produce them, fraudulent or otherwise, today, they essentially get you a job.

And the Social Security card as well as the driver's license is commonly used for a whole host of other identification purposes today. Yet, it is probably the most fraudulently produced document in America. It is a document that has been flimsy and paper for years. In recent years the Social Security Administration has put a few fibers in it, but by no means made it tamper-resistant or counterfeit- proof. And I encourage this committee and other members of Congress to really take a look at a proposal that I have in as a legislative matter for a good number of Congresses, one that is attached and submitted to this testimony today, H.R. 191, and a bill in the last Congress, Mr. Chairman, that you were an original co-sponsor of.

That is a bill -- that is a proposal that would require the Social Security Administration to make the Social Security card as secure against counterfeiting as the $100 reserve note, with a rate of counterfeit detection comparable to the $100 reserve note, and as secure against fraudulent use as the United States passport. Now, we're not talking about putting pictures on the card, we're not talking about any of that, but it's all those interweaving, interwoven things that you can use to -- use ultraviolet lights and so forth to determine.

I also would encourage the same type of activity that has been discussed here today with regard to the driver's license. I think that drivers' licenses, at least the general standards for what they are, should be uniform throughout the country, and I don't think we have to mandate that. I don't think Congress should pre-empt the states, but I think that there should be an effort to encourage that from Congress, and I think that it should be done in a way that does have either a uniform standard proposed, or you get the states together to do that, or whatever.

All drivers' licenses should certainly have photographs on them, they should have the signature on them, they should have a fingerprint or another biometric identifier on them. And they should have holograms and other types of devices built into those drivers' licenses, just like I suggested for the Social Security cards so they cannot be easily reproduced, and so that when you take it somewhere, to an employer or to a person who's in law enforcement, they can quickly be checked.

You know we have a little machine that's been around for a number of years on fingerprints. You put it on this desk -- I've had it when I was chairman come before my committee; you probably have too, Mr. Chairman. And it's doing

nothing more than saying if you put your finger on that machine and you put the card that you have with your pre-existing fingerprint on it, it matches it or it denies it. And it doesn't have to ***go*** to some central database to do that. At least that'll tell me biometrically whether the person I'm looking at is the same as is on that card.

I also concur with the view that we need to do something about birth certificates. One of the great, great problems in this country are the (breeder ?) documents Senator Simpson's talked about, and that's important.

Last, I want to comment on one aspect of the Immigration Service, because I do believe that the focus rightfully should be there, as Congressman Castle stated in his opening. There is a great, great opening right now in this country for people to come here and not be identified. We need a tracking system. We need to be -- we need to find people so we don't have visa overstays, and we need to shore up so many things.

A number of things have been mentioned, but one has not been. Today when somebody ***goes*** before a formal proceeding of an immigration tribunal, or to the Immigration Service or whatever, they're usually released on their own recognizance or maybe on a cash bond. The Immigration Service has the authority to have a security bond, much like a bail bond, but they don't do that.

And I believe that it would be extremely helpful to get people to show up when they're supposed to before immigration proceedings. If there was a general policy that a security bond be used and then have the private sector, bail bondsman if you will, like they do on criminal law, be responsible for bringing them in; making sure they do show up, because people can come not only into this country and get here too easily because the visa system and visa fraud and we don't track them, but then when they do show up to a proceeding and they're supposed to come back in 90 days or six months or whatever, we have no system to bring them back in, we have no way of knowing where they are, and we don't have nearly enough police or immigration officers that will ever be able to do that. So why aren't we using the private sector, in the same way that we do in criminal law? And it's not being done today.

So I would encourage that this committee and your members look at -- very strenuously at not only making these identifiers more secure and finding ways to track visa overstays and people who come in here, but making sure that when they're here, that is those who are aliens, show up when they're supposed to at the end of whatever period of time that there is.

Thank you, Mr. Chairman.

REP. HORN: Thank you for your testimony, and we'll now ***go*** to questioning. It's ***going*** to be five minutes per person because of the travel schedules, and we will alternate between the majority and the minority. And I'll start it off and it will be -- Mr. Chief Counsel, we'll get the technology here, we're in business.

In my opening statement I cited a few research center studies that showed overwhelming support, 70 percent of those polled, for a national identity system and are all of these people just misguided? How do you feel? Do you think, from what you've seen, does the average citizen when you get into a debate like this -- and I would take it with this particular three of you, would you have, say, a hardened, if you will, Social Security? Or would you take the license, which in my case with California they have a photo and they have a thumbprint. And not all of them do it, but that's pretty good identification.

So any type of -- other type you're talking about than simply hardening up the Social Security card, and then putting a picture on a it or a thumbprint? I remember when the supervisors at Los Angeles County, which is a county of 10 million people, and they started with the photo on the welfare situation and a few thousand people got off the rolls because they were ***going*** two, three, four places to get money, and that was one way to do it.

MR. WILLIAM MCCOLLUM: Well, Mr. Chairman, if I might respond?

REP. HORN: Yeah.

MR. MCCOLLUM: I don't believe that, for example, the Social Security card, you want to ***go*** to put a picture on it. I don't think you need to -- I think it can stay paper. Its purpose is to make sure that the number that's on that card and the name on that card are the bearers, and that when you take that card and produce it for whatever purpose that, that very simple fact can be verified.

I also think, by the way, that it would present problems in reissue, and so that the Social Security card -- one of the great reasons why that's been a problem in getting it corrected is the Social Security Administration won't ***go*** to the cost of reissuing a lot of these cards. They don't have to reissue all of them, but I do think they do need to reissue those with -- those with younger age group and they -- that would be an added expense that I don't think you would want to encounter.

And, again, I don't think we need a national ID card as such, a separate card, if you have the driver's license and you have the Social Security card, one with a picture, one without it, that are more secure, more tamper-resistant and counterfeit-proof.

MR. SIMPSON: It's interesting, Mr. Chairman, that polls throughout the select commission back in the '80s, '85, '90, if you'd asked the American people, Roper, Gallup, whatever, if they favor restrictions on immigration, 70 percent do. It just stays that way. Not illegal or -- I mean, I'm talking about legal and illegal immigration. Interesting.

But when it comes to the Congress it doesn't get done that way because the Statue of Liberty suddenly enters the phrase, and all of us are children of immigrants, mine from Holland; orphans. If my granddad hadn't killed a guy in the middle of the main street, we would have had a better reputation there in our state. But that's another story and I won't ***go*** into it.

(Laughter.)

Nevertheless, you can't continue to talk about the Statue of Liberty again. You must talk about reality, and all three of us I think are; all of you are. But I think the one that surprised me was when they put the examination into California for the written exam on truckers. Guys just stood outside the building because they didn't want any part of that, because they'd been using fake IDs and all the rest of it, and it was a very serious problem. And I think you ought to look into that California commercial driver's license issue, written exam.

MR. GINGRICH: I think that what you have to recognize is that the people most opposed to a national ID card are dramatically more passionate than the people who have some vague, general support for a national ID card. And that's why I think Senator Simpson was right early on in saying that if we ***go*** down that road, it's a dead end. It won't happen. On the other hand, most Americans I think can be led to agree that having an efficient transfer of information so you know that your driver's license is real, that it's valid, so you can check it across state boundaries and for specific purposes. Foreign visitors, I think most Americans would agree, you could have a nationwide system of identifiers, because that's not part of what we think of as our civil liberties.

People who have very important security jobs, whether it's on airports or elsewhere, people would agree you ought to have a pretty high standard of security, because they understand that that's a function of your job; it's not an infringement of civil liberty. But I would encourage you to be minimalist in this. You want to get to a highly secure system that is across the whole country, that is ideally mostly decentralized in terms of states implementing it but with information able to flow across state boundaries. And you want to do everything you can to minimize the threat to those whose primary concern is civil liberties.

REP. HORN: Thank you. My time is up.

Five minutes to Ms. Schakowsky, the ranking member.

REP. SCHAKOWSKY: Thank you, Mr. Chairman.

Following up on that minimalist approach and using your examples, Speaker Gingrich, of what happened before September 11th, that the CIA actually transmitted information to the FBI and it never got through. What I'm wondering is are there not systems in place, were we to have the proper technology for sharing that information, that could provide the kind of security we need?

Let me just -- that's the question, but let me just say that in many, many hearings that we've had since September 11th, we have found that information was all over the place and had it only been shared and gotten to the right place, that we could have done this or that to prevent what happened. And so I'm just wondering if it isn't a matter of looking at our systems, adding new technologies where we need to, but not new authorities to gather that information. If it's just a matter of making more efficient what we already have.

MR. GINGRICH: I think you're 90 percent right, but the 10 percent that's missing I think could kill us. Let me describe what I mean. First of all, whatever system we build, we ought to have a competitive team try to break, because -- to find out how rapidly can you buy a counterfeit? How rapidly can you figure out a way to work around it, because we have active opponents who study what we do and who can spend two or three years trying to penetrate our systems. And if we're really serious about security, then we ought to be serious about learning what its weaknesses are.

Second, as Senator Simpson said a minute ago, we discover that whether it is illegal aliens or it is people who are for one reason or another using a false identity, that there are, even in the current system -- even if you had 100 percent accuracy of sharing the information, some of the information ***going*** into the system is false. And we don't necessarily today have the kind of identifiers and the kind of structure that makes sure that the information you put in is accurate information. I think that would be the other zone where I think there has to be really serious work done. But I yield to my colleagues who know more about this than I do.

MR. SIMPSON: Well, Congresswoman Schakowsky, you are right on track. One of the most frustrating things for me, and I know for Peter Rodino (ph) and Ron Mazzoli (ph), Fish (ph), all the rest of us, was the absolute stubbornness of the agencies to share information. The one that appalled me was Customs and INS. Oh, there's a real internal -- it was bizarre; it was childish. Customs wouldn't -- you know, Customs can pick up a lot of stuff. They know what's ***going*** on and stuff coming in. And they'd share out and they'd say, we handle that.

The Border Patrol and the INS and the Justice Department and the CIA and the FBI and often times their arrogance, and the CIA's secret arrogance. I mean, this is where you have to smash the big bug, right here. And I think that's what I hear the president saying, that he's ***going*** to give Ridge all the authority to do that and he's ***going*** to make them do it. Well, we've all been here a long while. Merry Christmas, we'll see what happens.

(Laughter.)

MR. MCCOLLUM: I know that that's a big problem.

What Senator Simpson just said and we joked about it is so true. If Tom Ridge can do it -- I see the other day where he's talking about merging maybe the Border Patrol and Customs and maybe the Coastguard. I think that is ***going*** to be an awfully big hill to climb and that we'd be better off -- you'd be better off using the energies you've got to do things like forcing the Social Security Administration to really ***go*** out and make the card tamper resistant. Make it like the $100 bill. Take the driver's license, make it more secure. Take the ideas that Newt Gingrich just said about putting a database together nationally to talk to each other on these things, technically. Then cajole, continue to cajole the agencies to do this.

REP. SCHAKOWSKY: Thank you. Let me ask one quick other question. One of the problems created by driver's licenses becoming de facto national identification systems, is the privacy protection of those records is very poor. We know that states often sell that information along with the person's address and it becomes out there in the public. How can we make sure that any particular system we use doesn't mean that that information is sent out? And should Congress stop the validation of Social Security numbers until the states institute -- a state institutes

privacy protections for driver's license records, because they often check those drivers' licenses against the Social Security cards?

MR. MCCOLLUM: Well, Ms. Schakowsky, I don't think that we should stop the validation system as it exists because, you know, we've got a security problem right now. We need to let these things happen as best we can. But I do believe that Congress should be concerned and should encourage states to make the right decisions to protect the privacy of the data that's in the database. That's the real point I made about not wanting a national ID and trying to define it for you.

The thing the American public may say when they say, we're all for a national identification card, is one thing. But when they really get down to it, nobody that I know of favors a Big Brother database somewhere, whether it's in the state or in the nation, where other people can ***go*** and get access to your personal information. And there's a huge difference between providing a chance, for example, for somebody who's an employer or law enforcement to call up or do whatever we can on the computer, to a database and say if you walk in and this is my name and this is my Social Security card and verify that they both match electronically. There is a big difference between that and somebody walking in and saying, "Okay, I've got a name, now let me ***go*** find out -- what is the Social Security number, tell me?" Or the other way around: "I've got a Social Security number. You tell me the name that ***goes*** with it."

We don't want that information shared publicly, and that's the kind of thing that you need to discriminate, in my judgement, against. But you're not ***going*** to mandate that in one big piece of legislation. It's ***going*** to take a lot of work to get understanding on the part of each person or group in the states that are making those decisions, to make them be aware of what they're doing and to be more secure at educating them.

REP. HORN: I think the gentleman --

MR. SIMPSON: May I add one thing, Chairman Horn?

REP. HORN: Yes, ***go*** ahead.

MR. SIMPSON: Newt Gingrich is a wizard of the keyboard and I am non-adept in technical prowess of the electronic age. But I do share with you, I believe totally, there really is no such thing as privacy any more because of the information technology. They've got you in every database in this country: Social Security, driver's license, organ donor, blood type, you name it, FBI reports; I used to read them. And with what's happened with information technology in this country, I think privacy is ***gone***.

REP. HORN: I now yield five minutes to the gentleman from Florida, Mr. Miller, then Ms. Maloney.

REP. MILLER: Let me follow up on what Senator Simpson brought up, and that's the issue of privacy. I know Speaker Gingrich and Mr. McCollum worked this issue when they served here in financial privacy and medical privacy, and I know that Hugh Russell (ph) was trying to get legislation through. Would you comment on that experience and what the experience has been that you're aware of, controlling that kind of privacy? Because we are all public figures, and you all were certainly public figures when you served here in this institution. But that's really one of the core concerns: privacy. And when we passed legislation on financial medical in particular, is it working? And what can be done to make sure that we can ensure privacy if we move to some type of ID?

MR. GINGRICH: Well, let me say first of all I think this is an extraordinarily important issue. But in a way, big computers are a much greater danger than Big Brother. And it's partly true because it is so seductively convenient. You use a credit card. It doesn't occur to you how much information you're building on that credit card every week when you charge things, what it tells somebody who's clever about your habits, your interests, your tastes, et cetera.

Then you ***go*** and you use telephones, which have records. And then you ***go*** and you pump gasoline. And then you ***go*** and you get a driver's license. I mean, by the time you're done with all this, if you were to actually assimilate -- or

accumulate all the information that currently exists about you, you'd be stunned at how much you are a public person in ways you did not intend.

And I think there are two very different layers of this. We badly need to think through an integrated privacy policy in terms of law. As I said earlier, I'm a passionate believer in electronic medical records, but I'm also passionate believer in a federal law that will make the inappropriate misuse of that information a felony, and have very stiff penalties. Because I think we have to have the information, but we want to protect people from having it exploited to hurt them.

Similarly, I think that it's important to recognize -- and I want to -- as I started my testimony earlier, I want to commend this subcommittee again. You know from your report issued last week that the federal government agencies have security levels that in many cases are so laughable that any really competent sixth grader could break into them. And even the ones that are relatively secure, except for the top two or three, a relatively competent junior in high school could break into them.

And I think it's really important to understand that you've got -- and I met recently with the National Association of State Chief Information Officers, and we talked about the fact that we need to set a whole new standard against hacking, against organized crime, against terrorists, against foreign governments that want to try to break in, and recognize that that's ***going*** to take a sharing of technical knowledge.

It's not just writing laws, but it's understanding how to write the security systems. And we have to recognize how much of our code is now written outside the United States. And I think we have to have a project that the defensive and research project agency, and the national science foundation, and the national security agency, to really figure out a way to literally scan all the code we now rely on, because we don't know how many various back doors have been built in. Because you're talking about millions of lines of codes that routinely, now, enter the U.S. system from overseas.

MR. SIMPSON: May I say, too, sir and to the panel, who knows more about the loss of privacy than all of us? You, me; all of us who are in public ***life*** have none. And maybe that's all right. It's all right with me. I laid it all out there, all the peccadilloes and the goofy things I ever did. But there is no privacy for a public figure. And so I think it's very important to realize that as we do these things, the media loses a lot of sleep about us, because when we get active they ***go*** into everything we've ever done: first grade, high school, college, the whole works. And we get the whole load.

When you come back to them and say, "And aren't you intruding in our privacy?" and they say, "Well, you're public figures, we're not." I say, "More guys know you on that tube than know us, all of us in Congress, so don't give me that. I think we ought to know a little bit about your private ***life***." It's a sick idea, I know. It's about the First Amendment. It belongs to me too.

But this is really -- we're the ones that have suffered the slings and arrows. And I haven't the slightest -- I'm ready to do that at any time. In fact, anything, anything -- and the woman I've been ***living*** with for 47 years is sitting back here -- in anything they couldn't dig up on Al Simpson, but let me tell you, they've sure as hell tried.

MR. MCCOLLUM: If I might, I'd like to make a distinction. Mr. Miller, you've asked about privacy. And I think it is what is a person's reasonable expectation, what are the constitutional protections for that, and there are some. And we ***live*** in a different age when it comes to the computer, but we need to divide up what people should reasonably expect in the way of privacy with respect to their government intrusion, and intruding into that, and what they can reasonably expect when they ***go*** out and take certain steps on their own in the private world, in the world of business and what data that they freely yield to someone for a purpose. Two different things.

The privacy that's protected in the Constitution clearly is there when it comes to the government coming into your house, not just from a criminal law standpoint, but a reasonable search or seizure, or eavesdropping, or whatever, and we have all kinds of checks on that and they should always exist.

When it comes to the computer, when you use the computer, you need to just simply be aware you are opening up whatever you put in there to other people to look at it. And we can talk about trying to restrict that all we want, and it's very difficult to do. On the other hand, when you give up data, say, to a bank, which was where we first met the privacy issue in the last congress and it created a hullabaloo, I don't think people were even thinking about the privacy question so much there.

But the reality is that prior to the enactment of the big bank bill last Congress, banks could share data that they had with anybody. There were no restrictions. And we put the first restrictions. Congress did, and the law. And those restrictions said that since we allowed the merger of the operations of banks and security companies and insurance companies, that if you were in the same holding company, you know, the same group owned all three of you, within that group financial information that you, as a citizen, gave to that bank could be shared. But if they want to ***go*** out and give that information out to somebody that wasn't a party to their company, to their big, you know, their holding company, they had to seek your permission.

And those are the kinds of things we need to think about at each stage. You give up your rights when you ***go*** and do a certain business transaction, but you should be informed what you're giving up. And before information that's given by you to a business or third party is given away to somebody else, you should have the right to say yes or no. But, absolutely, you should have a reasonable expectation the government won't intrude in your privacy. That's sort of the broad guidelines. It's a huge subject. But that's the guideline. Thank you.

REP. NEWT GINGRICH: I thank the gentleman.

And now five minutes for the gentle lady from New York, Ms Maloney.

REP. MALONEY: Thank you, Mr. Chairman.

Speaker Gingrich, you mentioned that you were not supportive of a national ID card, but you supported a more efficient transfer of information. Since all of the known terrorists were visitors with visas here, either legally or illegally, it appears that a good place to start would be with a sort of smarter, a more thorough tamper proof Green Card. Would you agree?

MR. GINGRICH: Yes, I did say earlier that I drew a very sharp distinction between the need for a national system for non-citizens, which I think should be administered by the federal government, run across the whole system, should have a clear identifier that's biometric and should have a database that can be accessed by a variety of agencies. And that just I think should be a condition of being here.

I also said, and I think you'll get real controversy about this, that I think we are much better to ***go*** to some kind of guest ***worker*** program, and accept the legality of people who are here for the purpose of working and get them identified. I think when you have a pool of -- I think the numbers are three to five to seven million people, who are illegally here but are here actually to do legal things -- they're not here to be drug dealers, they're not here to be terrorists, that pool of people who are outside the system causes I think a real challenge for security purposes.

So I think it would be much healthier to have an identifiable guest ***worker*** program, and simply have a requirement that everybody who's a non-citizen have, as you said, some kind of identifier and a sophisticated Green Card with a central database. That should be national. And my guess is overwhelmingly the American people would support something like that.

I'm also suggesting if you come here as a visitor, as part of the transit point that we ought to have some biometric, I think probably an iris or retina scan, so we could determine whether or not you, in fact, are a person that is a threat to the United States. That is at a point of entry, even for visitors who are here on business or here for tourist purposes. And my guess is most people who are on the planet -- people who come for business or for vacations want to be safe, and they want a safe system. And as long as it's not too intrusive I think they'd be very accepting of that kind of safety.

REP. MALONEY: Building on that base of a non-citizen database that is national, who should maintain this database? Where would you put it in government? Would you put it in the INS? Would you put it in the FBI? Would you put it in the new Homeland Security? Where would you put it?

MR. GINGRICH: I'm ***going*** to yield to my two colleagues on this. I have actually not thought about where in the federal government you would house it. I would probably outsource a great deal of management of it, just because I think they -- it's very, very hard for the federal government to get first class --

REP. MALONEY: But it has to be maintained federally?

MR. MCCOLLUM: Well, it's the Immigration Service you're talking about. I don't know what -- (inaudible) --

REP. MALONEY: You would put it in INS.

Where would you put it, Mr. Simpson?

MR. SIMPSON: It was my experience, Congresswoman Maloney, that the -- I met some of the finest people in both parties who were commissioner of the INS. It is an absolutely unwieldy agency. Doris Meisner did her best. There's nothing you can do with them. The regional people are tough, district people. They're all -- it's got to be done there. I think that's -- if you ***go*** ahead with the legislation that's being proposed, then it would be the INS which would be logical, not Social Security. Something about Social Security remains rather sacred with --

REP. MALONEY: This is only for non-citizens?

MR. SIMPSON: Yes, indeed. Well, many non-citizens hold Social Security cards.

REP. MALONEY: I would also like to ask the panelists, who do you believe should have access to that database, assuming it's in INS with a recite by --

MR. GINGRICH: I think for verification purposes it's reasonable to ask people to prove that they're who they are when they apply for a job if they're a non-citizen. And I think I would allow law enforcement people to have access to the proof that they are who they are. Beyond that basis, I would say it would have to be on a carefully screened federal law enforcement basis. But I think if a highway patrolman pulls you over and this is part of your proof of who you are, it ought to be reasonable for them to have at least the negative access that says, yes, this is a valid -- this is a real person.

REP. MALONEY: Of the other panelists, who do you think should have access? Do you agree?

MR. MCCOLLUM: Well, I think that what Newt Gingrich is trying to say is very clear. I think he did say it, but I want to amplify it and that is that the key to all of this, in identification right now, and certainly in the area of these aliens that are here or coming here, is the proof that they are who they are, that verification.

That is that's the whole idea if you have a biometric where you can pick your fingerprint and put it here, maybe that ***goes*** back to some database where you corroborate, hey, that is Joe, you know.

But I don't think the general public should have access to it, and I don't think that anybody but law enforcement for very specific purposes, probably only Immigration Service and key law enforcement people, should have access to the full information; presumably the data on that alien about, you know, where they were born, how many times they've been married, that sort of thing.

REP. MALONEY: Okay, and my time is up.

REP. HORN: I thank the woman from New York, and now the only librarian in the history of Congress, Major Owens, and the gentleman from New York. Five minutes for questioning.

REP. MAJOR R. OWENS (D-NY): Thank you, Mr. Chairman. With this distinguished panel seeming to agree that the national identification card would not be a silver bullet, maybe we can put the argument to -- the debate to rest once and for all and focus instead on another problem that I think most of them would agree we have, and that's the problem of monumental mismanagement in our agencies. You know, the kind of mismanagement which allows us to have a worldwide electronic surveillance system that can pick up all kinds of information, but they didn't have enough Arab translators in the FBI and CIA to deal with the translation of vital information. I could not believe that when I heard it, you know.

Right now we have a recent airplane crash in New York and it appears that turbulence from a jet that took off just before is probably the cause of the accident that took place. After all these years of flying and jets we don't know about turbulence and what it might do to an airplane? Or, you know, the mismanagement is such that decision making within these vital agencies like CIA and the FBI is off to the point where Aldrich Ames could sit there for 10 years on the payroll of the Soviet Union, and Robert Hanssen to be on the payroll of the Soviet Union for 14 years.

Maybe your prestige and your influence can be put to work on a crusade to ***improve*** the management of all these. Our technology is excellent, you know, and way ahead of our capacity to use it. Including INS. The computers are always breaking down and there's always a problem, you know. If INS maybe had some of the budget of the CIA, a comparable budget -- $30 billion plus ***goes*** to CIA. INS is always struggling to just maintain enough staff to --

MR. : If I might --

REP. OWENS: Maybe I'll just conclude and you can comment. Maybe such a crusade by people of your caliber would get to the heart of the matter and all these other things would fall in place, you know. The credit card companies -- the companies that issue credit cards are very familiar with ways you can develop a foolproof card. They know there's no foolproof card, but a certain degree of fraud they put up with and -- but they're pretty much on top of it. Various ways to do it and some identification card consolidation would be very convenient for most of us -- you know, I think a lot of people.

But the real problem I think is a monumental mismanagement. I think the history of the fall of the American cyber civilization might be written one day and the cause will be human error. That's what we ought to --

MR. MCCOLLUM: Congressman Owens, one of the greatest frustrations I had in the last couple of years in Congress was the fact that over the years I had been one of those people who was beating up on the CIA and others to get more language speakers of Farsi and Pushti and all those languages that we're now seeing, we don't have. And we kept pouring money at it and they kept reporting to us and they kept not getting the numbers, and telling us they just weren't available. The reality of it is --

REP. OWENS: -- they had a lot of people spoke Russian and languages -- a lot of good librarians have worked for the CIA.

MR. MCCOLLUM: Well, it is a --

REP. OWENS: (Off mic) -- Soviet Union, but --

MR. MCCOLLUM: The problem is --

REP. OWENS: (Off mic.)

MR. MCCOLLUM: But my point to you, and you know this because you served with me in a number of these capacities, is that you sit there and you have -- you're only as good as the product or the effort of the person who's right in charge at the moment and the vision they have. And the vision in the case of some of these things, including the language issue you're talking about, had to be to ***go*** out and be creative and find that and get that language more quickly in place. It didn't happen.

The same thing is true about the immigration stuff we're talking about here today. That's why we all hope, and you do too, that some of the ideas being ***batted*** here today will really be enacted; that SIGMA (ph) and others will ***go*** out and do it, and we won't just be talking about it as we have for all those years since 1996.

REP. OWENS: We've had a problem with Arab terrorism since the Beirut bombing when President Reagan was president. Arabs, the World Trade -- you know, why after all those years don't they have translators who can translate documents from Arab?

MR. GINGRICH: Let me just say I -- in your five minutes you put your finger on the heart of the American challenge. In a sense, it's what Senator Simpson said earlier when he wished Tom Ridge luck as part of his Christmas present. And it ***goes*** to the core of whether we are a comfortable system or we're a serious system. The difference is a comfortable system accepts any innovation that doesn't require it to ***change***. So it gets to ***go*** on doing whatever it wants to do. A serious system says this is what has to happen.

If you watch Jack Welch at General Electric, for example. He's probably the best modern CEO. I mean, he said GE to be successful has to ***go*** and become X and that means we're ***going*** to ***change*** in the following ways, and he drove the ***changes***. Now, there are three problems: rivalry, bureaucratism, and acquiring new capabilities. Rivalry, as I think Senator Simpson was saying earlier, the CIA doesn't want to share with the FBI and the FBI doesn't want to share with anybody.

I mean, it's an absurdity and it should be a national scandal that the watch list didn't get through at Logan Airport after 42 days, as an example. The one that Senator Simpson mentioned. The Border Patrol and the Customs agents, standing next to each other, have different computers. Now, that's just a level of deliberate bureaucratic turf guarding that shouldn't be tolerable and that should be shameful.

Second, bureaucratism. I had staff at the American Enterprise Institute pull this up the other day. There are 51,000 Pashtuns in the United States. Now, if the Central Intelligence Agency can't find Pashtun speakers, they should assign someone to ***go*** to National Airport and wait for the taxis to come out.

(Laughter.)

MR. : Right. That's exactly right.

MR. GINGRICH: I mean, the idea you couldn't hire a translator who -- you don't have to ***go*** through the process of vetting somebody to be a FBI agent, or vetting them to be a CIA agent with secrets in order to have them as a translator. The notion you couldn't find an Arab translator in the FBI is -- it tells you how bureaucratic they were, how lacking in drive and seriousness, and how unwilling to confront reality.

Third, I mentioned earlier before you got here, as a librarian you'll appreciate that I'm ***pushing*** books. I mentioned Clayton Christensen's book on the innovator's dilemma, because he really makes the key point. Really big breakthroughs tend to come in really small companies. Just the nature of how breakthroughs occur. Government is peculiarly slow at finding those. Government procurement makes it almost guaranteed not to acquire the newest technologies.

And so I think you put your finger on a profound challenge for the American government. I wish President Bush well and Director Ridge well in trying to -- to try to get this thing solved. But I think you've absolutely described the core problem of us becoming an effective country in the next decade.

MR. SIMPSON: May I just say a word to my friend Major Owen, who I've enjoyed very much through the years. We've had some nice sessions together and traveled together. You're absolutely correct when you're talking about mismanagement. And then you're talking about the thing that all of us never do well, when we're here and it's called oversight hearings. We have an oversight hearing, we bring in an agency, they prepare for it. Oh, man, do they get ready for it, and then you beat 'em up. Everybody just beats their brains out from up on the panel. And they all say,

"Don't worry, we recognize that. We're ***going*** to correct it. We're so thrilled that you see too that this is a problem for us."

After pounding their brains in all day and after them slip, sliding along, like that old play, "The Best Little Whorehouse in Texas" where the guy just slid all over the place, we don't do anything. I couldn't do anything. I had oversight hearings with the INS and they told me the most magnificent things for 18 years and nothing was ever done. It was with violin music in the background and timpani and bells, you know. But it's oversight and that's the tough one.

REP. HORN: I'd better give you one more question. And in his testimony for the panel two, Professor Turley will propose that a commission be established to study the feasibility of a national identification system. What do you think of that proposal? You've been on these commissions. Should they do, whoever they are? Presidential and leadership in both chambers or have legislators ***go*** up to the trough and see what they can do?

MR. SIMPSON: I think a national commission -- I speak from experience -- this select commission did two reports on legal and illegal immigration by the Chairman Ted Hesburgh and both of the commission reports were enacted in the law. The essence of the legislation. So I think it's good. I do think that it has to be not called a national identifier. It should be called "how to make more secure the systems of identification and work recognition in America," or something like that. If you use national ID, it's over.

MR. MCCOLLUM: I believe, as Senator Simpson does, that commissions do form the nucleus and sometimes the initial impetus to get legislation enacted, when you need to get a consensus together, and I share his concern. The whole idea of a national ID, as I described it in my opening statement to you, Mr. Chairman, is a non- starter and we don't want to talk about it. Not that we don't want to recognize people could call something that, but I don't want a national ID with a national database with Big Brother. What I do want is the improvement that that commission could recommend and make things more secure in identification that really works in this country.

MR. GINGRICH: Let me be a doubter just for a second. I'm not opposed to a commission, but I think we know an awful lot of what needs to happen and Congress, I think, could move expeditiously early next year on an awful lot of stuff. Particularly, as it relates to non-citizens we really know how much we have to ***improve*** that system. And I'm not sure that we need to have more people tell us -- I suspect, if you had your staff from the Library of Congress pull up all the commissions on this topic in the last 20 years and simply put out a summary of recommendations, you'll be astonished how much already exists and how many smart people have already worked the issue. I think it's important to move while the public is paying attention and cares about this topic and that would be in the next session of Congress, not three years from now.

MR. MCCOLLUM: And by the way, I'd echo that. I think he's absolutely right about that point.

REP. HORN: Well, I thank you all for coming. I know when the three of you are together, it's ***going*** to be a lively session. We wish you well.

MR. GINGRICH: Thank you, Mr. Chairman.

REP. HORN: We'll ***go*** to the second panel now.

(Pause in proceedings.)

REP. HORN: Let's get them to take the oath also. So raise your right hand. Do you solemnly swear that the testimony you will give before the subcommittee will be the truth, the whole truth and nothing but the truth?

WITNESSES: I do.

REP. HORN: The clerk will note all the individuals, the witnesses -- and I didn't see too many other assistants.

So let us start then with Mr. Turley, Shapiro professor of Public Interest Law at the George Washington University Law School. Mr. Turley.

MR. JONATHAN TURLEY: Thank you very much, Mr. Chairman. First of all, let me express my thanks for appearing again before this subcommittee and also to appear before you, perhaps for my last time, as chairman of this subcommittee. We all owe you a great debt and your retirement is a real loss to this institution and I want to be one that thanks you for it.

REP. HORN: Remember, you're under oath now.

MR. TURLEY: (Laughs.) Obviously, this is a subject where generally more heat than light is generated and in a rare display of academic modesty, I will say that I will not resolve the questions surrounding this debate. I would, however, like to offer a constitutional historical foundation perhaps to move the debate from what is often kinetic rhetoric to a more stable basis for discussion.

It's certainly not enough to dismiss national identification systems, as opposed to a card, as unprecedented. The framers gave us a system that was certainly at the time unique, because it is the most nimble and versatile system in the world. As in nature, nations that fail to evolve are least likely to survive. The world is not static and so our responses have to be as dynamic as the world around us. So this is a hearing that is looking at a question that's very much a question for our times. Whether you consider the national identification system to be a necessary security measure or Big Brother's little helper, we need to reach some type of consensus. And so tonight, I'd offer my views on those lines.

Today's debate is part of the long, unbroken debate that has raged between the government and the governed. We, as Americans, have a virtual hereditary suspicion of government. As Oliver Wendell Holmes said, "The ***life*** of the law has not been logic, it's been experience." And our experience with the government, in systems of this kind, has not been good. It's been long and painful. We have learned that government authority operates along the same principles as a gas in a closed space. As you expand that space, government authority will expand as well to the full extent of the expansion. And from Biblical times, and I've laid this out in my written testimony, through the Ottoman Empire and Henry VIII to the present time, nations have tried to create national registries. Not for oppressive reasons but for necessary reasons. But those systems have, as we know, been used for great harm.

Now, we also need to get away from a habit of talking a good game about national identification systems. We are very proud, as Americans, that we don't have human license plates. But the fact is we have a national identification system; it just doesn't happen to be a very good one. We have allowed the Social Security number to mutate into a national identifier. That is ironic since, as I mention in my testimony, the Congress was quite clear that the Social Security number was not to be used as a source of identification. This Congress has repeatedly said that it should not be used as opposed to a national identification card. And so the question is: why in my wallet do I have a drivers license, a smart university card, an athletic card and credit cards that are all based on my SSN?

Why do I have two kids, one who's three and one who's one and a half, who have their own cards? They are already being tracked. Human serialization that we fear is here in some respects. But the reason it's here and the reason we failed in our efforts to control the SSN is because the market had a need; it created a vacuum that in the absence on Congressional involvement, it filled that vacuum. The SSN was inevitable because the market needed it.

I happen to have a great deal of problems with national identification systems. I tend to fear government, quite frankly.

I tend to like at least of it as I possibly can have. But we also have to be concerned that if we do not act, that the market will act for us. We have to be concerned that if we remain passive, there will be efforts to fill that vacuum, and they're happening right now. At this moment, the heads of Department of Motor Vehicles have already moved

towards a -- what's called a de facto national identification card. The airlines are working on a fast track card of their own, that will effectively have a national footprint.

Now, I don't know the heads of Departments of Motor Vehicles, quite frankly; maybe I should. But I don't they're the ones that should make this decision. I think that you're the ones that should make this decision and it's important for you, I believe, not to be repelled by the idea to the extent of being absent.

I happen to believe, and this may disagree with our earlier panel, that we may want to discourage the development of those cards. We may want to try to exercise some degree of control as to what is happening in the country in terms of identifications. If nothing else, to avoid the creation of redundant systems where we suddenly have a whole bunch of cards that become barriers to travel.

Now, in the review of identification cards around the world, you have over 100 nations with different cards. But to use the term national identification system, let alone national identification card, is virtually meaningless. These systems are unbelievably diverse. Some of them are really little better than our SSN system. Others are incredibly detailed and are attached to databank that probably would make most Americans feel uneasy.

But using the reference to Nazi Germany and to the abuses I think is a little bit overblown, but it is relevant. It is overblown in the sense that we have a nation that has its own safeguards, constitutional safeguards, cultural safeguards, that make those types of abuses of historical but not contemporary relevance. Many of our friends around the world, like Belgium and France and Germany, are great democracies and yet they have these cards. So I think we need to look at this with the appropriate amount of passion, but also with an open mind.

Now, the cards differ of course dramatically. Britain of course had a national identification system that was discontinued in the 1950s, when they had a negative ruling by the Lord Chief Justice. They're now considering a new card. And they range -- we can look at, for example, the Belgium identification card, which is one of the most developed of systems. And in Belgium you are required to have a card at age 12 and then you're required to carry it by age 15. You are required to have it on you. It is not an internal passport system in the most negative sense, but it is a potential barrier in the sense that when you ***go*** to an airport, apparently, in Belgium, you do have to show the card. Obviously, Belgium has not used that card for oppressive means; far from it. They have a large database that the police have access to.

Germany also requires the carrying of a card and it has a great deal of information, it's incorporated into a database which is accessed from multiple sources. Like Belgium, it's a stand alone system. Other countries like -- for example, for the Dutch they have the SOFI number, which is a more developed system than our Social Security system. It's sort of a hybrid between these various options. And you can ***go*** through, as my testimony indicates, from country to country to look at all of these options.

Now, as we move towards to a national identification system, if we are ***going*** to move towards that, then we need to look at the constitutional and legal parameters for that system, because we're all talking about so far a system more of authentication. And it seems that we're mainly talking here, and the members have already indicated, they're interested in authenticating people, to make sure they are the people that they say they are.

So we have to distinguish between what we're trying to achieve. Are we trying to get a ready identification that's reliable for the cop on the beat, so that he can take a look, and a card is biometrics and other elements that make it hard to tamper with? If that's the case, the card could be largely contentless. It simply requires those biometric elements to be reliable as authentication. If we're talking about, as has been discussed in the past, a smart card attached to a database, we're talking about a far more significant issues in terms of constitutional and legal questions.

One of the most important constitution questions that have to dealt with is the right of travel. The Supreme Court has said that the right of travel is virtually unconditional in the United States. And when we develop national

identification systems, we have to be concerned not just in drift, but that those systems can create barriers to travel that will impinge upon that right. And I ***go*** into that in my testimony.

We also have to be concerned about creating a national identification system that will fall into the trap of the Brady Law. To some extent, any national identification system will require the integration of state and federal systems. To the extent that we commandeer the state agencies, we're moving into a separate area in which constitutional concerns would be heightened. Then, finally, there are privacy protections that I talk about in my testimony.

What I would like to propose is that Congress consider one thing that I think is clear, and clarity in this matter is truly valuable. It should not necessarily be clear how we should proceed, but it should be clear how we should not proceed. We need to look at the SSN experience and not repeat it. That's not how we do national policy. We allowed the SSN to be propelled into a national identifier, without any vote of this body. There were a couple of laws in which this -- in which Congress embraced the SSN. Franklin Delano Roosevelt wanted to use the SSN, but for the most part this has been done with little foresight and control. And as we see these, quote "de facto identification cards" in the making, it seems that history is repeating itself.

So that's the reason I've recommended the creation of a federal commission and, God knows, this town does not require another commission. I've been on a federal advisory group. I was on it for three years and at the end I wanted to take a ballpoint hammer to my head. They are frustrating, there's too many of them, but unfortunately I think this is an area that deserves a commission; unlike the ones that we have seen in the past.

Newt Gingrich is right, we have had commissions in this area, but none have been given the specific task of looking at whether we are ***going*** to have a national identification system. Whether or not we act or not, that's important. We need to have a commission that looks at the question of whether there is inevitability, whether in this information age we're ***going*** to have this Cosian (ph) problem where the market is ***going*** to dictate those conditions unless you do something. So we have to deal with reality and if that reality is that businesses and agencies need national identifiers, I would rather have you involved in it than the hidden hand of a market which may take us away from privacy.

That commission can look at some questions I've laid out in my testimony. The first one is what the function utility of a national identifier card is. I've already mentioned that, but there are vast differences and when you look at what people have said about national identification systems, they are as different as you can possibly be. Some of them are talking about massive databases; some of them are talking about immediate authentication. I don't know which one we need, but we need to look at that before we do anything.

Second, we have to look at the utility of the system. Part of the problem with a national identification card is that you can have a sleeper agent from Al-Qaeda or an espionage agent in the United States. One of the most effective ways to penetrate a nation is to have a sleeper and he or she comes into the country, she has a wonderful ***life***, is a wonderful neighbor, ***goes*** to PTL meetings and then about nine years down the road Al-Qaeda activates her. She's got a wallet full of every possible card, from the PTA to a fast track card, to a national identification card.

Finally, we need to also -- I'm sorry, second we need to look at what technology would be used for the system. We have everything from iris recognition to DNA fingerprinting to facial recognition systems. We need to look at those technologies. We need to, if we're ***going*** to embrace the technology, embrace one that is ***going*** to be good 10 years from now, that is ***going*** to be accurate and reliable. We need to look at the system to prevent hacking, because if this is ***going*** to be a system like Belgium's where you need it to get on a plane, then frankly it's dangerous to have the usual government error rate with databanks and databases.

Finally, we need to look at what type of protections we need to put in place. As you know, the Census Bureau information is supposed to be private but it was used to round up Japanese Americans. We also know that information from states has been sold on to private companies. And then, finally, I've suggested that we consider the need for a constitutional amendment. I have never supported a constitutional amendment until this year. But there is a trend that needs to be arrested and that trend is the diminishment of privacy. It's chilling to hear a person

like Simpson, who I have a huge amount of respect for, say that privacy is dead -- because if privacy is dead, we have allowed something that is uniquely American to die with it.

So in conclusion, the test of the moment, I think, is to try to protect our society without ***changing*** it in the way that we lose the object of our defense. The framers never said this would be an easy road, they simply said it was the only road for a free people. And so I suppose the charge of the framers is this: how to keep us safe from harm but to pass along our system to the next generation with the condition it was passed to us? I think that's a subject that deserves some thought and circumspection. I thank you very much for your time today.

REP. HORN: We thank you very much for your presentation. I have had the opportunity last night to read all of them and we will first get all the presentations, then the members will have a question and answer with you and dialogue.

Now, my next witness here we deeply are for, Roy M. Goodman, state senator New York. You joined us on such short notice. We thank you very much. You flew down here from New York this morning after our invitation yesterday afternoon, so you get things done very fast. And I look at this background. Any legislator that has 1,200 of his bills become law, that's impressive. So we're lucky around here if we get five to be presented. And we thank you because you are also in the same business we are as chairman of the Senate Committee on Investigations, Taxation and Government Operations, and looks like you've had a lot of fun. So thanks for coming.

MR. ROY M. GOODMAN: Mr. Chairman, thank you very much indeed for that warm welcome. I'm grateful to you and the members of the committee for an opportunity to appear before you today, albeit on relatively short notice.

I would like to make at the outset a comment of warm salute to my former colleague in the state Senate in New York, Major Owens, one of our more esteemed members who has risen to the heights of the U.S. Congress.

Major, I can see just from the height of the ceiling in this room that we have pygmy proportions compared to the stature which all of you possess and I'm very proud to know you.

And also Ms. Maloney, who happens to be my own congresswoman. I very much hope she'll be around in a few moments so I can salute her personally, a much esteemed and good friend; although on the other side of the aisle, I must confess.

May I say, Mr. Chairman, that once upon a time on the matter of personal identity there was a gentleman who entered his men's club -- an elderly chap with mutton-chop whiskers, a typical old Peter Arneau (ph) personality -- and he sunk into a deep chair and rang the little bell next to it on the table, by which he hoped to summon the club's steward so he could order his usual martini. Nothing happened and he rang the bell again. Finally, after ringing it four times, he was outraged and someone came by and he said, "Great God, man, do you know who I am?" and he was speaking to one of the employees of the club. And the chap looked at him and said, "No, sir, I don't. But if you'll ***go*** down I'm sure the gentleman at the front desk will be able to tell you." So this was an indication of an identity crisis that occurred under slightly different circumstances.

May I say, sir, that on a much more serious note, unfortunately I appear before you at a moment when the nation is plunged into a war which it did not seek and which was visited upon us in a most astonishing fashion on September 11. The trauma of that is simply indescribable. I might just tell you that on my second trip -- my first trip down to Ground Zero I had a chat with the fire commissioner, who was describing some of his experiences on that particular day. And without being too lugubrious, let me say that he said a chap came up to one of his firemen and said, "I have a helmet here, sir." And he said, "Why are you bothering me with that? We're trying to save ***lives***." He said, "The reason I'm bothering you with it is that there is a human head in the helmet."

Alas, the gentleman had been decapitated and this was one of the horrific, horrendous things that occurred on that date. And, needless to say, this is something which has embedded itself in all of our minds most profoundly, and

with a sense of deep grief and outrage we appear before you to discuss the problems relating to the identity card matter. And I have to tell you that my whole view of it is heavily tinctured by the fact that we are at war.

I spent three years in the Navy during the Korean War and wore about my neck at that time an ID tag with a thumbprint engraved upon it, so that the idea of having a fingerprint identification is certainly nothing new. My officers' identification card had a full set of prints on it. It is something which anyone who's been in the military services is fully familiar with.

I thought it would be useful just to take a moment to review with you the contents of my own wallet in regard to cards. I confess I hadn't thought to do this until I sat down here this afternoon, but I notice that I have a few of them. And just to give you some idea of the extent to which privacy is invaded, let me give you a quick inventory of my cards. I'll make it very brief.

On top is a picture card identifying me as a New York state senator. Beneath that is my drivers' license, which also has a picture of me upon it. My Citibank Visa Card which also has a picture on it. My MTA, that is to say Metropolitan Transit Authority subway card, which has my picture on it. A Sam's Club card, Sam's Club being a retail establishment where I have credit, which has my picture on it. And then we ***go*** through a series of others: American Express, New York Society of Security Analysts, my Medicare card, my New York Public Library card, my Wyoming Public Library card, where I ***go*** in the summer time, my Barnes and Noble credit card, my New York government employee benefit card, my Automobile Club of America card, my Metropolitan Museum identification card, my Whitney Museum card, my Museum of Modern Art card.

That is just a few of the things that I carry with me to be sure that I am at all times able to identify myself as I ***go*** about my daily routine. I think this gives you a little idea of the lack of privacy which we have, even with the best of intentions. We are certainly photographed widely and our data is on file in many different places. I'm sure anyone in the room could produce a wallet with somewhat similar credentials and make the point that we are today certainly in an identification card society at a very broad level.

And may I say to you, sir, that it had been my opportunity as chairman of the Investigations Committee in 1993, when the World Trade Center was bombed -- you may recall we had a dreadful incident in which there was a gigantic explosion. I ***went*** into that hole and found a tremendous crater five stories deep and three stories high, and at that time felt it important to examine the matter of how we have achieved security in regard to the terrorist possibilities of future attack. And we prepared a report at that date stating that there were many vulnerabilities and we thought it advisable to create a commission, which commission would have as its principal objective eternal vigilance to try to prevent the recurrence of this type of terrorist attack.

In so doing, I'm sorry to say that people's eyes quickly glazed over and, as is our want as human beings, we fairly soon forgot that episode. And not until September 11 when we had this far graver problem arise with such unpredicted suddenness, did we find ourselves in the position of having to once again reconsider this. And I did pull together a group of five former police commissioners, groups from the FBI, from the Ports Authority, police and a number of others to participate in an examination of potential terrorist targets and possible means of defending against them.

That committee happens to have issued a report yesterday which I have and have, I think, sent in advance to you. I won't attempt to touch on all aspects of it, because it ***goes*** far beyond the subject of today's meeting. But let me say that we believe that there are at least 50 different ways in which we should be tightening up the security in the state of New York to prevent future occurrences.

They cover such things as commercial airline safety, private airline safety, which is a thing that has loopholes the size of the Lincoln Tunnel. Anyone can ***go*** to a private airport, get on a plane of almost any size, load it with any cargo without any inspection whatsoever, proceed to fly over the United Nations building, fly into it and destroy it in a matter of seconds, in much the same fashion that the World Trade Center was destroyed. And the same would apply to the Empire State and others of our magnificent buildings in New York.

So that this just indicates the extent to which in this war time environment we have not really risen to the concept that we must gird our loins and prepare ourselves with emphatic dedication. I think it was Herbert Spencer said it was only by iteration and reiteration that we impress an alien conception upon an unreceptive mind. And it's only by iteration and reiteration that we must remind ourselves that we are at war, and war is a very grim business in which we have to suspend values which we normally might wish to feel are repugnant to us in other contexts. I see my sign has just signaled stop.

REP. HORN: Don't worry. Just keep ***going*** a little.

MR. GOODMAN: Thank you, sir. I'll try to keep it as succinct as I can. Let me simply say to you that with regard to the matters of other emergency issues, we've looked at hospitals, we've looked at the transit system and at various matters relating to nuclear electric gas supplies to the city of New York. There's a possibility that our power could be shut off very simply by ***going*** to a point of convergence of electric lines. We want to emphasize the problems of biological and chemical warfare, about which much has been unfortunately discussed here in Washington in the wake of the anthrax scare, and on and on.

And let me say that I speak at the moment on behalf of my colleagues who are former police commissioners, as I've said, including the new police commissioner designated to the city of New York, designated by our new mayor. His name is Raymond Kelly (sp) and he is an expert in the law and, indeed, I think is a man of balanced judgment. It was the unanimous judgment of this group that there should be instituted a national identification card system, and opened questions whether it should be voluntary or involuntary, and I'm not prepared to give you any conclusion. My colleagues are thinking on that.

My own concerns at the moment are very great. As a civil libertarian of long standing, I'm very much concerned about the possibility that such a system could be misused. But let me just say that we now have the -- as Mr. Ellison has pointed out to us, the means by which to create cards which can carry a tremendous amount of information and certainly establish beyond any reasonable doubt the identity of the individual holding the card.

As you may be aware, in Israel people ***going*** seeking entrance to an airplane do not have to stand on long lines. They ***go*** to a kiosk and insert their card, insert the palm of their hand and stand in front of a camera, which does three things, I'm told. One is to check whether the palm print coincides with the print on the electronic chip embedded in the card, to determine whether the facial characteristics are such as to be individual involved. And, finally, to determine whether the retina of the eye, which apparently is unique in every human being, is such as to positively identify the individual. This tripartite identification concept is one which is now technologically feasible and is in effect in various countries around the world, and has been used quite successfully.

So the question is not whether it can be done, nor is it necessarily the cost of doing it, because one could envisage a system in which there are payments made as a service, as we pay for EZ-Pass cards in our cars ***going*** through the toll facilities in New York. So that I'm simply here to say to you that the problem becomes one of the extent to which this could impinge upon privacy. And I'd remind us all that the Supreme Court has stated unequivocally that there is clear protection in the law for privacy, but not for anonymity. And there's nothing about any Supreme Court dicta of which I'm aware, and this point is fully emphasized by the distinguished civil libertarian lawyer Alan Dershowitz, who in a paper made it clear that, in his judgment, the time had come for the use of these cards.

And I say to you, sir, that it's my belief that in order to accomplish several objectives the cards may serve a useful purpose and I'd like to quickly outline the objectives, and that would conclude my testimony. The principal purpose of the card would be to positively identify an individual, to be certain that his identity has not been stolen. As you may know, identity theft is a matter that is now quite pervasive in our society. People's identities have been stolen. Their bankcards have been lifted. They've been charged with purchases which they never made, telephone calls which they never placed, and the like. So that there is a serious problem of finding a stable means of positive identification which, as I've indicated, now exists.

So that the question then becomes one of whether we are in a position to use the cards constructively. I would say to you that for the privilege of not having to wait two to three hours on an airline counter line, that that might be worth a $25 payment for a lifetime or a two or three year subscription to a card. Similarly, I think it's quite clear that this would eliminate the need for profiling, an obnoxious thing based upon ethnicity, or the various other characteristics which have been used by police to properly identify presumed suspects.

By having a positive ID card, a man could walk in wearing all sorts of outlandish clothing with a beard of three feet long and side burns, and all of the things which might normally be associated with someone who is an undesirable, by virtue of easy thinking. And by simply presenting the card, he would exempt himself from the need for any special profiling type examination. It strikes me that at this moment, because of the unique facial hirsuteness of the people with whom we are at war, that there is a problem. As you recall, a Hindu was mistakenly taken for a Muslim and slaughtered early on, right after September 11, which is the kind of tragedy we certainly wish to avert. And an ID card would preclude that type of problem altogether, it's my judgment.

Furthermore, there are various conveniences if one wished and wished to volunteer to have certain health aspects of one's existence on the card. If you dropped to the ground with a cardiac arrest and the card were in your possession, it could be put into a reader and quickly determine your condition of health and whether certain drugs could or could not be administered to you, whether a defibrillator would be an appropriate thing to use in view of your heart rhythm pattern and the like, and this could be a very beneficial health aspect to the card system.

So the point that I'm making is that it's not simply an intrusion of privacy that's involved. There are various collateral benefits which should be weighed into total consideration of whether these cards make sense. Mr. Chairman, let me just sum up by saying that it's a complex question and because of my civil libertarian concerns I've thought long and hard about this. I do believe at this time we have the sufficient sophistication and awareness of the types of problems that exist to form a decent judgment in the matter, and I would respectfully suggest to this committee that it take a very close look at least the volunteer use of such cards.

I think at this time, in view of our war emergency, they've become very relevant to attempting to determine who is improperly in the United States at any given moment, tracking people who may be undesirable or have patterns of sabotage or other behavior which needs to be properly overseen and tracked, and that without such cards it becomes exponentially more difficult to accomplish this purpose. So with those thoughts in mind, I shall now subside with all due respect and thank you very much for a chance to be heard.

REP. HORN: I think you mentioned earlier that you had some recommendations out of your committee, and once you're done with it if you could -- we'll have a spot in this to get the whole document.

MR. GOODMAN: I'd be glad to do that.

REP. HORN: Thank you very much.

MS. MALONEY: Personal privilege. I would thank you.

REP. HORN: He says he likes you.

MS. MALONEY: Well, I would like it if you'd welcome my senator, actually.

MR. GOODMAN: (Inaudible) -- and I took the liberty of saluting you most warmly.

MS. MALONEY: (Inaudible) -- for many, many years. And we welcome your testimony. You've always tackled the hard problems and come up with good answers, and we appreciate your distinguished input into this committee. Thank you for coming. It's good to see.

MR. GOODMAN: Thank you very much. It's good to see you too.

REP. HORN: We now ***go*** to Katie Corrigan, who is the legislative counsel on the privacy issues for the Washington National Office of the American Civil Liberties Union. And she has quite a background in terms of health, education, labor, pensions matters. And we're glad to have you here.

MS. KATIE CORRIGAN: Thank you. Thank you, Mr. Chairman, and thank you to the members of the subcommittee. I appreciate the opportunity to testify before you on national ID proposals on behalf of the American Civil Liberties Union. The ACLU is a nationwide non- partisan organization with nearly 300,000 members dedicated to protecting the individual liberties and freedoms guaranteed in the Constitution and the laws of the United States.

Like all Americans, the ACLU supports efforts to ensure our security from terrorist threat. But we remain convinced that we need not sacrifice our liberties to protect our safety. We believe a national ID system in any form should be rejected. First ACLU believes that the threshold question is whether or not a security measure would be effective at protecting us from terrorist threats. Since the terrible events of September 11, there have been numerous proposals to create a national ID system. The rationale is that we need to create a clear line between us, the innocent people, and them, the dangerous terrorists.

Every one of us would like an ID card that would put us squarely on the right side of the line and exempt us from suspicion and heighten security when we board a plane or ***go*** to work. Unfortunately, none of the proposed ID systems would effectively sort out the good from the bad. An identity card is only as good as the information that establishes an individual's identity in the first place. It makes no sense to build a national ID system on a faulty foundation, particularly when possession of the ID card would give you a free pass to board a plane or avoid security checks at federal buildings or other public places.

No form of documentation is completely foolproof . The same people who are forging IDs today will forge them tomorrow. There are always ways to beat the system. Presumably, an individual would obtain an identity card using a document such as birth certificate or a driver's license. Anyone, including terrorists, could alter or obtain such documents. The inspector general of Social Security testified last week that six of the hijackers obtained Social Security numbers through fraudulent means. And, as U.S. citizens, domestic terrorists like Timothy McVeigh would certainly qualify for an ID.

Second, not only would a national ID create a false sense of security but it would be very, very expensive and divert resources from perhaps more effective counter-terrorism measures. In 1998 the GAO reported that the Social Security Administration estimates no matter what material a card is made from, or what type of technology, including biometric, is used for security, issuing an enhanced card to all number holders using current procedures would cost a minimum of about $4 billion or more. And even with the offer from Oracle and Larry Ellison for free software, the processing costs alone of issuing new IDs to Americans are estimated to be 90 percent of that billion dollar expense.

Third, in addition to huge costs, a national ID would require a massive identification bureaucracy to support it. Thousands of government employees would be required to develop, implement, maintain the supporting computer infrastructure and technology standards for the ID card. The SSA's $4 billion estimate didn't even consider the cost of updating the picture or other identifiers on the card over a person's lifetime, or periodically replacing the magnetic strip on the back, or the simple cost of having to replace lost or stolen IDs.

When setting up any new bureaucracy simple questions need answers. What would happen if an ID card is stolen? What proof of identity would be used to decide who gets a card? What would happen if you lose your ID? Anyone who has had to correct an inaccurate credit history will understand how hard it could be to correct an error that has found its way into a government database. Error rates in government databases already tend to be especially high, and we heard that from members of our first panel.

And what happens if you are misidentified, or one of the thousands of victims of identity theft? Even with a biometric identifier on each and every ID, experts say that there's no guarantee that individuals will be identified or misidentified in error. A technology expert at the University of Pennsylvania recently said biometrics are fallible.

Fourth, an ID system violates basic American values, including our privacy, equality and our right simply to be left alone.

Day-to-day individuals could be asked for ID when they are walking down the street, applying for a job or health insurance, or entering a building. This type of intrusiveness would be joined with the full power of modern computer and database technology. How long before office buildings, doctor's office, gas station, highway tolls, subways and buses incorporate the ID card into their security or payment systems? The result could be a nation where our citizens' movements inside our own country are monitored through what would equivalently be internal passports.

The database supporting such an ID system would be massive and contain all sorts of highly personal information. Thousands and thousands of government employees and even private industry could have access to it. The scope of information accessible through a centralized database, as opposed to the many different databases that are attached to the cards that Senator Goodman pointed to, would magnify the risk of privacy violation.

One mistake by a government employee could result in disclosure of personal information that could follow you around the rest of your ***life***. This past month a state university accidentally posted the psychological records of 62 children on the Internet: names, addresses and along with intimate details, such as a boy prone to anger outbursts, gender identity issues and bedwetting. Disclosures could come back to haunt children later in ***life*** when they are trying to find a job or get a security clearance. With an ID system, one accidental keyboard stroke could put a person's most sensitive information into public distribution.

And finally, Mr. Chairman, some people have argued that ID would end racial profiling and other discriminatory practices. Unfortunately, we believe that cards would provide new opportunities for discrimination and harassment of people who are perceived or looking or sounding foreign. The 1986 requirement that employers verify the identity of potential employees and their eligibility to work in the U.S. has resulted in widespread discrimination against foreign-looking American ***workers***, especially Asians and Hispanics. A national ID card would have the same effect on a broader scale. Latinos, Asians, African Americans and other minorities would become subject to more and more status and identity checks. This would have a stigmatizing and humiliating effect and undermine our right to equal treatment.

A national ID system in any form would be expensive, require a cumbersome bureaucracy and violate some of our fundamental American values. And it simply wouldn't work to stop terrorism. The ACLU urges the Congress to reject proposes for a national ID system and I'd be happy to answer any questions at the appropriate time. Thank you.

REP. HORN: Delighted to have your presentation and we now move to Rudi Veestraeten, the counselor and ***consul*** at the Embassy of Belgium, and he's been in their Foreign Affairs Ministry in their home city and he's had a -- he's had quite a career for his own country and we're thanking you for telling us how that works.

MR. RUDI VEESTRAETEN: Thank you, Mr. Chairman. Thank you, members of the subcommittee. It's an honor to be invited here today. I'll try to give some comments. I had a document, which was distributed, contains the basics about the system in Belgium.

First of all, Belgium is -- for those who would doubt -- is a democracy. It's a democratic country. We have a longstanding record of democracy and -- and that is the specific -- we have a very longstanding record of registering people and issuing ID cards. We actually started issuing ID cards in 1919. We started registering people locally in towns and in cities in 1800. That is an existing system in Belgium.

I think when we talk about ID cards, when we talk about registration, there are -- and talk about the events of September 11 and other threats in the society today, there are in fact three elements which are often mixed. First there is the ID card as such. ID card is just a document which allows somebody to authentify (sic) who he is. A hundred years ago, 50 years ago people might still just know you and know who you are. Even today people in my village in Belgium, they know who I am. My neighbors here in McLean, they know who I am.

But when I drive around in a car, people do not know any more. The card is just a means to prove who you are, that you are who you say you are. That is the card. Then there is the second element in this discussion: the database issue. We also have a quite sophisticated system in Belgium with a centralized database which contains a limited number of informations. You can find that in the documentation.

The database is a very powerful tool to quickly find more. If somebody shows up and has an identity card, you can then as a police officer, as a public servant, depending on what your duties are, you can then find out about that person what is his background. These are data not contained in the cards, not written on the cards, but there is a whole database behind the card; a system where more information is available if needed and to those who need it.

And then there is the whole issue of security. I'm not ***going*** to talk about that, but that's a whole other issue. Of course, the fact of having a card, having a passport, having a travel document, having a driver's license does not allow any police officers to determine whether a person is a terrorist or is a genuine person. That's not a purpose of the card. Let's not mistake this. The purpose of the card is just -- is only to authentify that this person is indeed -- does have this first name and that last name and is properly registered at a particular address.

This is very important distinction to make, I think. If we discuss about the abuse of cards -- I mean, the threats of having cards in a country like Belgium, the threat of having this system where everybody needs to carry cards. Well, in fact, you can say the same -- this dates back from the German occupation. We were occupied by the Germans twice: in '14/18 and in '40/45. We have been fighting the German system, the German the Nazism, the fascists, in '40/45. We are proud to have done that. I think we have a longstanding record of fighting authoritarian mechanisms, authoritarian regimes and we are very proud of that.

Now, the Germans, when they occupied Belgium they used police -- they used military police, they used an army to occupy our country and to take away all our civil liberties. Now, this does not mean that we have decided, after we were freed from the German occupation, to abolish police, to do away with an army, to do away with military police. That's not to the point. What we should try to do is to keep steady democratic control over what police does in our country. Keep steady democratic control about what the army is doing, what the army can do, what the powers are the army can be given. And that is the sense of the -- it's not about having police which can, of course, abuse its force; it's about control of the police.

The same ***goes***, in our view, in Belgium for the cards. It's not about the cards. It's about how you use the cards, what you allow people to do with the cards, the way you control, and so on. That is the essence of the debate in our country where it was taken.

Now, if we want to see what the card means in our system today, what do we use it for? I think the best way to -- and for the two ministers that have left, to explain that is to see -- to imagine -- from my viewpoint, for me to imagine my country without the identity card. What would be different if we would take away the identity cards in Belgium? I think first of all we would do what is the case in many other countries. We would probably see other documents being used instead of an identity card. This might be drivers' licenses, this might be Social Security cards. We have those cards in Belgium as well.

The problem there -- and that is why we have introduced the card in the first place, the problem is that those other cards contain data which are not meant to be communicated to some persons. I mean, on a driver's license there can be data which are not meant to be communicated to a bank employee. It can be medical data, like vision. It can appear not to be very important, but the vision is mentioned on the driver's license. Same ***goes*** for handicap in some cases. I mean, driver's license are meant for other purposes than identification, and therefore contain other information which are not meant for public distribution, and not meant for the bank employee.

Same ***goes*** for the security -- the other cards, Social Security card here and in Belgium. Those cards are not meant for identification purposes and so do not contain the proper security features which would be required for an identity card, which is a different issue. A passport is an identity travel document, so it's more similar to an identity card.

And then there is also the fact that some people might not have a particular type of card. They may not have a driver's license. I have colleague ***diplomats*** who do not drive their own cars. They do not have a driver's license.

So what do you do with those people in Belgium, if you would generalize the driver's license to be used instead of an identity card? You would then have to find a system where you would issue driver's license with no right to drive a car for identification purposes, which is not really what it's about. So that is one thing. We have a feeling in Belgium that the inappropriate use of other identifiers is in fact a highly sensitive civil liberties issue, because you would then abuse other cards. And information contained in other cards in other systems abuse this information for just mere authentication and identification.

What would also disappear if you would take away this card, and this is probably typical for Belgium and not for a country like the U.S., is that it's very convenient for people. We can travel in Europe with the ID. We do not need passports to travel in Europe to countries like Turkey, neighboring countries. We have agreements there. So if we would abolish the card in Belgium, much more people would need passports and this would increase the cost as well for those people as for the administration to issue all these extra passports.

In case of police checks, if some things happen and people are stopped in the street in a car, the fact that we have the identity cards and a very efficient database does save a lot of time. People can be released after only two minutes, just checking if this person is really who he is. So it's also a matter there in our view of civil liberty that we can release people immediately, if there is no need to keep them. We don't need to take them to the office, to the police office. Another very convenient use of the card is in case of unfortunate accidents. When there is an accident with a person on a bicycle, and he carries his cards, it's very easy to identify him to warn his family members.

So it's also in the advantage of the citizens of Belgium that the card exists. And then an alternative from this, we also quite generally use the identity cards to fight credit card fraud in Belgium. In many shops when you want to pay with a credit card, you would need to show your identity card, and the way you would show --

REP. HORN: Your time is running.

MR. VEESTRAETEN: Thank you.

REP. HORN: Thank you very much. We're ***going*** to recess now, because we have to get through the testimony and I want to give them full reason, Mr. Hoechst and Mr. Shneiderman. So we're in recess until 12:45, and in other words a quarter of one. We have a motion on the floor to recommit with instructions and a passage situation. So we're in recess until 12:45.

(Recess.)

REP. HORN: The subcommittee will be in order, and the recess is adjourned. And we will start with Mr. Veestraeten, who might not have been completely finished.

So you're certainly welcome if you want to give a few sentences on it.

MR. VEESTRAETEN: Yes, sir, I was finished. Thank you so much.

REP. HORN: Okay. We will then move to Mr. Hoechst, senior vice president of technology, the Oracle Corporation.

Thank you for coming.

MR. TIM HOECHST: Thank you. Mr. Chairman, Representatives Schakowsky and members of the subcommittee, on behalf of Oracle I would like to thank you for inviting me to participate in this discussion. I would also ask that my comments and written testimony be submitted to the record, along with an article written by our CEO Larry Ellison --

REP. HORN: Without objection.

MR. HOECHST: (Off mic) -- Thank you. The reason that I ask to do that in particular, is the article in its original form makes arguments about this issue that unfortunately were culled out during the endless number of editing processes that ***go*** on as articles reach sound bites. And so I think many of the issues that are relevant to this discussion, which I'll address in my comments, were part of that original proposal as well.

As we know, information is an incredibly powerful tool and whether we're using it to make decisions in a boardroom or on a battlefield, whoever knows the most about their situation is the most well prepared to make competent decisions. And in the country today, whether we're in the government system or in the private sector, we have countless databases with all sorts of information being gathered as part of the everyday processes of modern ***life***.

And the challenges associated with providing broader access to this information is exactly what we've working on for the last several years. But the reality is that knowledge that's culled from these databases, is not about the data itself; it's about the relationships that exist between data. And, as was fairly thoroughly discussed I think in the prior panel, in our opinion the real challenge is not creating new databases based on these various systems. It is coming up with a standard and secure and consistent means of establishing relationships between these databases when it's relevant, sharing information across these organizations, whether they reside within a single agency or across agencies, or even into the private sector.

So when we talk about a national ID card, I really think what's important to remember is it's not about the card. The card may -- we'll see in my comments in a few minutes, may have some interesting capability to make the process of securing our systems more convenient and more straight forward. But what we really want to focus on is the relationships between critical information systems. And in the example that was brought up earlier regarding sort of what was known about the people before September, the terrorists involved with the events of September 11 before the fact versus after the fact, point readily to this point.

After September 11 the FBI was able to discover a great deal about the people that were part of this act. The challenge was not that that data did not exist. We know the data existed because we know they gathered it after the fact. But the point was that we were unable to establish relationships between those pieces of information to make competent decisions. Now, we can make decisions after the fact, but this is the difference between investigation and prevention. And so if we are able to address the idea that through a common way of identifying people, inside information systems and standards for sharing that information between system is adopted, then we have a much greater opportunity of taking advantage of all the information that we're already collecting, when it can still be used to make a difference.

Now, if we think about the technical approaches with consolidating databases in this fashion, there's lots of different things we can do. First, is the idea of consolidation. We could start to bring together information systems from various organizations, even inside agencies or, more importantly, across agencies into huge monolithic government managed databases of everything we know about people.

This is not only a poor idea, it's not possible. Even if -- whether it's technically possible aside, it's socially not possible. The inertia that exists in information systems and inside organizations and overcoming the challenges of getting those organizations to roll up their information into systems that they don't control, is really a task that would be very difficult to accomplish; not to mention the fact that the government ought not be in the business of building huge consolidated databases of information about people.

Instead, we could decide that it's more important to keep these information systems separate, and let them do what it is they do today -- and they are already, like we said, gathering all sorts of information -- but create some standard ways for them to share that information with one another. And this could very reasonably be aided by a common identifier of people. So if we said between system A and between system B, whether that immigration and FBI, or an airline company and FBI, to validate that these two -- that we're both talking about the same person. Having standards for doing that could be very helpful in making that sort of communication more facile.

There are also other approaches which are not for consolidation or full distribution and connectivity, and this comes in the flavor of what I call sort of consolidated indexes of information. So for example, when a police officer pulls over a speeding motorist and wants to check for outstanding arrest warrants, does it make sense for that officer's system to check every ***local*** and state law enforcement in the country in real time, to discover whether there are outstanding arrest warrants? Of course not. Maybe it would be prudent for us to have a national system that points to outstanding arrest warrants. Again, the government not managing them, but the government providing a more convenient way of checking across systems that really do the same thing. And in fact the Department of Justice has implemented just such a system for that problem.

So the reality is all sorts of these approaches, when we talk about the consolidation and sharing of information, will be part of the ultimate solutions. We will have opportunity to consolidate systems that currently are duplicating effort. We'll have opportunity to teach systems that don't communicate with one another to do just that, and we'll have opportunity to create hybrids, assuming of course, that we come up with some standard methods for doing that.

The challenges in this are -- fall into two buckets. First, the technical challenges. The use -- the real challenge with an identification system like this is not just relating two people and two information systems; it is associating a human being with a given identity. How do I determine that this person standing in front of me is the same person I'm talking about inside this information system, or collection of information systems, and that identity comes through many of the ideas discussed today, maybe in the form of a card, maybe in the form of biometrics. Creating a secure and consistent biometrically enabled identification card that anyone could use to establish -- to authenticate identity would be difficult: not only difficult socially but difficult technically. The state-of-the-art here is advancing but it needs to advance further before we could turn such a system on in the short-term.

However, there is great opportunity for us to take incremental steps in attacking the technical challenges. First, in establishing standards for national identity, an identifier that uniquely identifies people and government guidance that should be used when building information systems related to these issues could be done incrementally and systems could come online as they choose to start to exploit such an identifier. We also talked about making the existing identification cards stronger rather than trying to establish a new one and there I think that the drivers' license is a good candidate for that because we've seen a lot of work already done there.

And then finally, in introducing specific populations to this technology rather than saying everyone has to participate, maybe we first focus just on critical jobs, people, for example, whose job requires that they are on the tarmac at an airport or specific populations of people, non-citizens visiting the country, for example. So from a technical perspective as a technology company and representative of that I would like to suggest that with the competent use of existing technology we can ***improve*** the security, not only of identifying individuals, but of establishing relationships between information systems that already exist today.

On the social side it's not so clear. And as the debates have ***gone*** on today, the issues related with privacy and the whole idea that the government is getting into the gathering and establishing a large, centralized databases, is an important debate but, honestly I believe that it comes down to the difference between can we do something and should we do something. The ability to do this and strengthen security is there.

The decisions as to when this should be done falls in the hands of policy-makers like yourselves. So it's important to remember that at discussion of whether we should do that has to be built on top of the ability to say that we can do that and for that "should" part of the debate, I think it's most appropriate to leave it to policy-makers to draw those lines of when such a system should be exploited.

So, given that, I appreciate your time and your opportunity to let us comment into this debate. Thank you.

REP. HORN: Thank you.

And our last presenter is Doctor Ben Shneiderman, Professor, Department of Computer Science, University of Maryland at College Park and he also here is a Fellow on behalf of the Association for Computing Machinery.

Thanks for coming.

DR. BEN SHNEIDERMAN: Thank you, Chairman Horn, for the opportunity to testify at this timely and important hearing. I want to commend you, Ranking Member Schakowsky, the subcommittee members and your staff for turning Congress's attention to proposals for a national identity card system. You've given some of my introduction already and I'll just say for further purposes that my statement represents the Association of Computing Machineries Committee on U.S. Public Policy. The ACM is a nonprofit educational and scientific society of 75,000 computer scientists, educators and other computing professionals from around the world, committed to the open interchange of information.

In the two months since the deplorable acts of terror were perpetrated against America, a number of legislative measures and regulatory actions intended to ensure the safety and security of our citizens have been proposed. While most proposals have been well intentioned, some have been misguided in that they overlook the potential for unintended consequences or underestimate the technical challenges and risks inherent in their implementation.

Recently information technology vendors have suggested that a comprehensive national identity card system could be created and implemented in as little as 90 days. Implementing such a complex system is a challenging systems engineering matter. Such a rapid construction of an effective and novel socio-technical system would be unprecedented. A constructive alternative may be focussed efforts that build on existing systems such as state motor vehicle, passports and visas, and as the last speaker I have the luxury of being able to resonate with the many thoughtful comments that have been made already. The first panel made very clear the strong political concerns about a national system and this panel has ***gone*** through in good detail about some of the challenges and technical development.

A national ID system requires a complex integration of social and technical systems, that's what I'm ***going*** to stress here is that combination, including humans to enter and verify data, plus hardware, software and networks to store and transmit. Such socio-technical systems are always vulnerable to error, breakdown, sabotage and destruction by natural events or people with malicious intentions. For this reason the creation of a single system of identification could unintentionally result in degrading the overall safety and security of our nation because of unrealistic trust in the efficacy of the technology. The national ID card itself is only the most visible component of a system that would require supporting bureaucracies and elaborate databases that would have to operate in everyday situations, again as said by several members of this panel.

In particular, a national ID system requires an extensive database of personal information on every citizen. Who would enter the data, who would update it, who would verify it, who would determine when the data is no longer trustworthy, who would review audit trails and ***improve*** access? If new and centralized approach is technically problematic, as again, has been stated by many, and politically unpalatable, which seems quite well accepted here, then how might we work to increase security? Constructive first steps would be to define goals and develop metrics of success. Let me repeat that: constructive first steps would be to define our goals in a narrowly, focussed way, and develop the metrics of success.

If ***improved*** air travel safety is at our goal and it has wide public support then we need to develop the techniques to achieve that goal with modest impact on personal rights and privacy. A realistic goal would be to make verifications of passenger identity more reliable while limiting delay, intrusion and inconvenience to citizens. ***Improving*** state motor vehicle identification cards might be accomplished by coordination among the states to determine best practices for issuing, replacing, verifying and monitoring usage. Such efforts might be coordinated by the National Association of State Chief Information Officers as mentioned by Newt Gingrich, or by the National Governors' Association.

Common practices or even national standards might be arrived at through public discussion. Adequate public discussion of proposals is essential to gain acceptance and to ***improve*** their quality. A socio- technical systems approach would include quantification of weaknesses and vulnerabilities of database security and network access based on existing systems, then realistic solutions to dealing with problems such as lost cards, mistaken identifications, would have to be developed and tested. Special cases such as tourists, professional visitors, foreign students, would have to be addressed.

Any complex social technical system such as identity verification requires well-trained personnel whose performance is monitored regularly. Effective hiring and screening practices, chances to upgrade their skills and especially participation in the redesign of the system are important contributors to success. Improvements for citizens could also lead to higher data reliability and system efficacy. Citizen confidence and data accuracy could be ***improved*** by system designs that provide greater transparency, greater openness, by allowing citizens themselves to inspect their contents and view a log of who uses their data. More constructive ideas could emerge by encouraging research by computer and information scientists in collaboration with social scientists. They would also be encouraged to build bridges with legal and policy groups so that their solutions are realistic and implementable.

It's important that Congress proceeds cautiously on the issue of national identity card systems. They involve risks in a variety of practical organizational and technical challenges. Any effort to ***improve*** homeland security should begin with clear statements of goals and quantifiable metrics of success. Computer technology can do much but it cannot see into the minds and hearts of people, nor can it replace the capability of vigilant citizens. Face to face security checks must be a vital component of airport and other security systems. At this point I also differ from Mr. Goodman's report about Ben Gurion University where -- Ben Gurion airport where it is not a biometric system but it is repeated face to face encounters with security checkers who ask questions and are vigilant to the responses and the behavior of each person passing through that airport as I did late in August of this year.

Despite growing public and political pressures for perceived security enhancements, the risks and challenges associated with a national ID card system need to be identified and understood before attempting deployment. But constructive alternatives, such as ***improving*** existing state motor vehicle registration and passports, are promising possibilities that could bring benefits sooner than establishing an entirely new system.

The emphasis must be on people first, then the technology. The Association for Computing Machinery, and other leaders in the computing community are ready and willing to assist lawmakers in their efforts to enhance the safety and security of our nation. Thank you for the opportunity to speak to you.

REP. HORN: We have been very enlightened by your presentations. I had a chance to ***go*** through them all last night. Except for the senator who is flying down here, I thank you, again. Would you object, I'll just ask all of you, would you object to a form of identification that contained only the person's name and confirmation that he or she is a U.S. citizen? How do you feel about that? That's getting down to essences.

MR. HOECHST: I think the issue is not just the card. Again the card is only the most visible form, but who issues the card, who certifies its correctness, and how it's handled. And my belief and my testimony suggest that strengthening existing systems such as state motor vehicle systems would be the most effective. We currently have accepted practice of walking up for airline boarding to show a state motor vehicle card. I think that is the place of intervention where we could do most good to ***improve*** its efficacy.

Simply creating a new card with whatever is on it, will lead us down the wrong path.

MR.?: I would add on this, Mr. Hoechst. Yeah, I would add that a card that just has a small amount of information, and really even perhaps less than you described, which can only establish identity is the only thing that is feasibly possible to deploy practically. Any attempts to create cards that contain lots of information just opens the troublesome box of discussions about how that information is used. What's important to remember is that the information that will be used once identity is established is already managed by processes inside organizations, whether they're law enforcement organizations or commercial organizations. What the card can only do is help

establish identity, authenticate that this person is this -- represents this sort of well understood and standard identity.

REP. HORN: Mr. Veestraeten, how do you feel about that, get it down to the name, and are you a U.S. citizen or aren't you?

MR. VEESTRAETEN: Yes, Mr. Chairman. That is exactly how it is organized in Belgium today. The cards only -- I added a copy of the only card which I had at hand, which was my own, with documentation, which has disappeared. We only mention limited number of data. This number is limited by law. So nobody can add any additional information. You will see on the back of the card there are two informations mentioned, and this is on my explicit authorization. I had to sign the documents to approve those mentions.

One is the name of my spouse, which I'm happy and proud to have her, and the other one is the number of the national register which is a single database. And I also approved in writing to have this mention added to my card. If not, it would not have been there. So the only information we have is -- we standard put on the card: name, first name, date and place of birth, and the address and the nationality, and there's nothing else there.

REP. HORN: Ms. Corrigan.

MS. CORRIGAN: I think that in order to answer that question, the Privacy Act, which was enacted in the 70s, was rooted in a golden rule essentially, which is that information collected for one purpose should not be used for another purpose. And it's difficult to answer your question because information is rarely collected just to collect it. There's usually a reason that you want to have such a list. So for example, a list of American citizens. And I think you yourself proposed something similar a few years ago around the voter registry. You know, the difficulty there is the same debate that came up around number one, as Professor Shneiderman pointed out, you know, do we have in fact an accurate list that would reflect that?

We do have the passport document only in the country, which establishes citizenship obviously. So there are documents that are shown to do that. ***Going*** back to one of my original points is that to build any one of these databases on a faulty selection of documents is very problematic, particularly when we're denying either a service or a right that you've got, either under a law or the Constitution.

REP. HORN: Senator Goodman.

SEN. GOODMAN: I'd like to reiterate once again the notion that in a wartime situation you have criteria which I think differ materially from those of the halcyon days day that we knew before September the 11th. And in this instance the purpose of the card would be to determine the -- to establish clearly and unequivocally the identity of the individual. But let me point out that at that stage of the game you have linkages with various databases, which might ascertain the possible undesirability of that individual's behavior pattern, which will require close tracking.

For example, if someone enters the country in a situation where they're here to do mischief, as it all too often in the recent past to be the case, it's imperative that we have some means of tracking that individual, to have a society in which everyone can rattle around in a state of happy anonymity and the assumption that the cool air of freedom must the thing which we permit them to breathe continuously while we're at war, I think, denies the exigencies of the war situation.

REP. HORN: Professor Turley.

MR. TURLEY: Well, I suppose I should be delighted about the opportunity to lie about my weight, but I don't think that this is an issue that will be solved by more cards. God knows, Senator Goodman's wallet couldn't hold another one. But I think my problem with it is simply that in simply having a card issue on an expedited basis I think puts us on a track of where we've been. That is, there is a natural desire to rush in this room and put this fire out. But I think it needs more study than that.

I think, not just because of our traditions, but because we have decided on the technology, its use, its functions, its appropriate functions, any dangers of what's called authorized misuse. All those things we have to think about before we plunge into this. I do think that there is a basis, as I say in my written testimony, to issue a card relatively quickly for certain insular groups. Those may be foreign nationals. They may be foreign students. But they would also be for example, international truckers. That we do need a very fast system at our borders that's reliable, because we have a build-up at our borders that's ***going*** to get worse, particularly during times of crisis.

We need to solve that right away. And we could create a biometric card to try to do that. We may also want to use the card for example, groups that handle material like anthrax. So you can have an immediate card issued. But what I think we should be careful not to do is to restrict it from drifting. Not make it a national card. Focus on those areas we need one right away, then study the issue of whether we need a national identifier.

MR. SHNEIDERMAN: Focus systems will be most effective and most prompt, I believe, in producing the benefits that we all seek. For, whether it's airport personnel or truckers, we can ***go*** and more groups can be approached and handled in a respectful way.

REP. HORN: I tried out on our first panel the idea of a commission which was usually a presidential commission of picking the chair and then the speaker of the House, and then the majority leader of the Senate. And I'm inclined to put that into law and have my colleagues with it. But what that does is delay things. On the other hand, what it does is try to build a consensus. So we had the Hesburgh one on immigration, we had Barbara Jordan as the chair, and so forth.

Now, we've been through this in terms of census material, where we wanted to put through a five-year or so, and they blew it right out because they didn't want any part of it. And it became a jurisdictional argument. So I'd be interested in what your feeling is. Is it worth getting a commission that has those suggestions, the speaker of the House and the majority leader of the Senate, and the minority leaders of both Houses and the president of the United States? What do you think?

SEN. GOODMAN: Mr. Chairman, let me suggest, it does not seem to me that that approach does take into account the concerns which we feel are increasingly evident, and I am afraid that if we are once again hit with another act of terrorism, which in my judgement is in all probability likely to occur sometime between now and Christmas, it's ***going*** to create the same reaction, only on an exacerbated basis that we had after the World Trade Center and Pentagon episodes. And I must say to you, I think that it's extremely important that we move on with this fairly quickly, and try to arrive at a conclusion. I would hope that some form of identification could be established promptly, so that we are protected to the extent possible against the recurrence of this type of an act.

On a lighter side, I am reminded of a couple on the Atlantic City Boardwalk, the gentleman got on the scale, put a quarter in and one of those little tickets came out with his fortune on it, and his wife said, "What does it say?" And he said, "It said that I'm a handsome, a debonair fellow with extreme brilliance, with the highest IQ in Atlantic City." And she said, "Well, let me look at it." And when she looked at it, she said, "Got your weight wrong too." So with the -- we do have occasional confusions in these mechanical devices, but I think we're at the point where that type of thing is not likely to occur with any frequency.

REP. HORN: Ms. Corrigan.

MS. CORRIGAN: Well, it sounds like the legislation does not have the ACLU chairing the commission, so it would be much easier for us to come out --

REP. HORN: Well, we don't know. I mean to say, you're here, and --

MS. CORRIGAN: Hey, I'm available --

REP. HORN: Yeah, and there are minorities in both chambers.

MS. CORRIGAN: I mean, I think the key is not whether there's a commission or whether it is staff on the committee developing a legislative proposal, I mean the question is what's in it. And, as you know, the ACLU would oppose an identification system, either through the front door of calling it a national ID, or through the back door of some other type of registry or integrated database.

REP. HORN: Mr. Veestraeten. Anything that Belgium ever had, say a Kings Commission, or the parliament, whatever, to get this moving?

MR. VEESTRAETEN: No, this dates from long back in our country, so I don't know how it was discussed back in the beginning of last century, but

REP. HORN: In the First World War and the Second World War.

MR. VEESTRAETEN: The card was introduced after the First World War.

REP. HORN: Yeah.

DR. SHNEIDERMAN: I think they have 80 years of history of evolution to develop their approach, which fits with their national values, and I think we've got a history of evolution here, and I support the idea of a continued evolution to refine the existing mechanisms.

REP. HORN: Mr. Hoechst.

MR. HOECHST: Mr. Chairman, I would suggest that your concern about a commission delaying things implies, especially with the ID card, that there is an opportunity missed that could be done in the short term, and so what I would suggest is that for the issue of identification cards, then something that studies that in the form of a commission would be valuable, as long as it were giving guidance that along some of the ideas that were proposed today, that it not just study it, but that it practice it, maybe in prototypical form, giving identification cards to different populations to see how it works, rather than just study it.

But I would also suggest that there is short term activity that can happen that I would hate to see a commission cause us not to focus on, and that is, on these goals of information sharing, especially between critical information systems in the area of law enforcement, and immigration and the like, where we do not -- the technologies exist, we know they work, we need to choose to use them, and we need to set clear guidelines about when it is appropriate to use them and legal to use them.

REP. HORN: Thank you.

Dr. Shneiderman.

DR. SHNEIDERMAN: I repeat my desire for the evolutionary, but I think also focussed action, as I say, as we hear it here, may be specific interventions between -- for information sharing between FBI, CIA, if our concern is aircraft and boarding aircraft, then that kind of sharing of information is a possibility in a very short term basis, and then I think focus populations, such as international truck drivers or airport personnel who have access to secure areas, immediate improvements could be made. But again, I want to restate it's not just building some technology, it's providing the human infrastructure that builds trucks and support for this, rather than antipathy. It must be demonstrated that any intervention has broad support, and especially of those who are most directly effected, but it's implemented in a way in which people feel that this does contribute positively and therefore they are most cooperative with it. And they will point out -- they will be vigilant in pointing out those who are potentially you know, in violation.

REP. HORN: I thank you, and yield at least 10 minutes to the ranking member, the lady --

REP. SCHAKOWSKY: Thank you, Mr. Chairman. I think this has been a really important and a very useful hearing. I think all the panel members, these are questions that we are ***going*** to have to seriously consider.

I want to first play a kind of devils advocate and -- because my proclivity is to be -- those of you who heard my opening statement, is to be very, very skeptical of the notion of a national identification card, but I -- the point that Mr. Veestraeten said, which is that we use identity cards, and all of you -- we do that when you ***go*** on an airplane, when you cash a check, all kinds of places where we do -- we are asked and required to produce some sort of identification.

It seems to me, if the technology is available to make -- to ***improve*** on those systems, maybe not perfectly, but to ***improve*** on those systems, then he asked the question, or at least made the statement that since we do that anyway, why not have a universal card, a national card. So, Dr. Shneiderman.

DR. SHNEIDERMAN: Again, I think that the warm support of participation from citizens is necessary. If they see that there's a universal card collected by a federal agency, I think the resentment may, and the doubt and the question, the interference of privacy would be very much on their mind. So you'd have a poor participation and I think disruption, people would be concerned. Whereas, if they applied for their state motor vehicle license, where they recognize that the benefit is they're receiving a card which enables them to drive, that it possibly takes care of health problems should they have an accident. And that there may be other specified focus clear benefits to it, they will cooperate, and that those who take the information will also have a clear sense of purpose and work as best as they can to ensure that the quality of the data is high, and that customer satisfaction is high, and that participation is broad. And again, when someone is attempting to forge or bypass the system, there's likely to be stronger civilian citizen participation in stopping such intervention.

I think we have the interesting examples of computer viruses. Why is it that the Linux communities or the Mac communities have less of this. There's a warm sense of participation, there's an active sense of pride, it's close to them. And so I think, if we follow those models and we want to bring, as in this country, we have a long history of bringing things closer to people by having the states be the closest point of connection for such activity, will be building the right kind of system. And thinking about the social dynamics of why someone offers their information and why they might try to deceive, and how they might help to prevent others from deceiving, that's where we will ***go*** to build the strongest possible system. So, again a diversified system and again a focussed one that deals with special communities.

MS. SCHAKOWSKY: Ms. Corrigan.

MS. CORRIGAN: Yes, I think here, whether it's a state level document like the drivers license, whether it's a Social Security number, or a newly issued type of identifier, like a biometric, I think again we have to ***go*** back to the purpose for which we're gathering this information. And the way that this debate has been framed since the terrible events of September 11th, has been a national identification card, or some sort of national ID system that would protect us from acts of terrorism. And, based on the arguments I already made in my testimony, we can't build such a system on a set of faulty documents. Many of those terrorists on September 11th had fake Social Security numbers. Actually all 19, according to the inspector general last week, had those security, some of them legally, and some of them not. And number two, ***going*** back to a comment someone made earlier, you can't establish motives or intent, simply on the base of knowing who someone is. And it makes me quite nervous to think that by having a traveler's ID, or by having some other national ID card, I could just pass through security unchecked, without much more.

And that to me doesn't create more security, and in fact creates a false sense of security: too much dependence on technology.

So I think, and whether we're talking again about state or federal level efforts, we have to ***go*** back to the basic question: is this even an effective security measure to begin with?

MS. SCHAKOWSKY: Is anyone else burning to respond, because I do have another question. Okay. Let me ask you this: is there a place for these incredible new technologies, biometrics, palm, all of those things. I mean, should we be looking for ways to utilize them more effectively, or do those lead into problem areas for us as well? Anyone? Yes, Mr. Hoechst.

MR. HOECHST: I would suggest that there is a great many places for using them, but not necessarily should we have an expectation that tomorrow we could use them to uniquely identify anyone who is on our soil, American or visiting. And that partly comes in limitations of the technology in its current state. But it partly comes just in the broad ability to adopt any sort of technology like that.

However, there are opportunities to use them where they are very effective. And this comes in, for example, authenticating yourself to secure areas. Perhaps, we'd say, you need to identify that you have certified -- we need to identify biometrically that you're allowed to enter secure areas at an airport or whatever. And for that sort of smaller focussed identification we know there's a subset of people who are allowed to do this, and we're ***going*** to confirm that you are one of that subset. They work quite well. For the general case of just saying, "Hey, I've got a person here. Let me look through all people to determine whether this person is this person," they are still maturing in that space, I think.

MR. SHNEIDERMAN: I want to confirm that on the technology side. These are promising technologies, but do not offer short-term hope for wide-scale decimation. We've heard in the past, voice recognition patterns and other technologies that might have been used. And these techniques are potentially interesting. They should be expanded. They should be researched, but they are in the longer term, and should not offer -- should not be seen as a techno-fix in the short-term.

MS. CORRIGAN: And, coming from the ACLU perspective, although they we're not the technology experts that you've got to at the end of the table, you know, I think our monitor is -- not all biometrics are created equal, and not all uses of biometrics are created equal. We apply the same tests to those measures that we would to a national identification card. And in the air security context the ACLU came out in support of the use of strength and identification cards for air employees that need access to secure areas, including the use of biometric on some of those cards.

The reason is that in those instances it's a limited and targeted use of the biometrics, and also you're able to take the thumbprint, or you're able to take the iris scan under very controlled conditions, which makes a difference in the effectiveness and error rates of biometric technology.

SEN. GOODMAN: Can I venture a comment if --

REP. HORN: Sure.

SEN. GOODMAN: I'm not sure at the moment whether we realize the extent to which certain technologies are already in plane, in attempting to achieve security. I'd like to give you a couple of quick examples in this regard. As you may know, there's something called CAPS, which is an acronym for computer-assisted passenger screening. This is a system under which information is obtained in the reservation process to screen out passengers who may require additional security checks. The airlines are fairly widespread in their use of such a system.

Also manifests are at this time provided by airlines. A manifest is a list of the passengers on a flight which would be landing in due course at a given airport. And in that airport, they receive an advance copy of the manifest or the list of the passengers on board, to try to determine whether there's a possibility of either customs violations or immigration violations and the like. So already Big Brother, if you please, is watching very closely, in certain instances, to try to determine what's ***going*** on.

In my judgment these are both fully justified under present circumstances attention and I would again repeat that in the context of a war situation, anything we can do to utilize current technology would assist us in making

identification of high-risk individuals as helpful. Normally you would not wish to do that, and you'd say, in a civil libertarian sense, case, they are surreal. Let it be, and don't mess with this sort of thing. But I think it would be a great mistake when we know that we probably will be, once again, subject to a potential attack, to allow ourselves to be in a somnolent in regard to matters of this sort.

MR. TURLEY: Could I add something? Obviously, I suggested a commission because I think this deserves more study. And I think that it's not just a technology issue that needs more study. But we need to look at the efficiency and viability of the system so that we can have a single unified card. It has to be integrated very often with at least some level of database that creates its own issues. But putting that aside, I just want to disagree a bit with Senator Goodman on one sentence.

And it's -- I happen to think that we do need more security. But we have a long history of the government in times of crisis, doing things that can only be described as moronic. And some of them are more than moronic, such as the internment of American citizens of Japanese origin. To simply say that we're ***living*** in danger is not a justification for ***going*** boldly into these areas in the search for even a modicum increase in security. I think we've learnt too much in terms of our history.

So I agree with Senator Goodman. I know that he intends this in the best sense, but I don't agree that should be the reason or the time schedule for us to add. I don't even believe as much they're ***going*** to add security. I mean these hijackers on September 11th have wallets that were bursting with false IDs. Adding another one is not ***going*** to reassure me. I would rather be reassured from my sons that when they inherit this country and this system that it's ***going*** to be given to them in the same condition that it was given to me. And that's my greatest concern because, frankly, the Taliban is today's flavor of threat. And tomorrow there's ***going*** to be another group of fanatics. But I'm more concerned in how we respond to a threat than the threat itself, at the moment.

MR. GOODMAN: May I remind us that had we taken the view that people's activities in the country are their own business unless they do something overtly wrong, that this possibly was what underlay the fact that we failed to realize that people were taking flying lessons learning how to fly planes in mid-air but neither to land them nor to take them off -- to permit them to take off. And had we simply accumulated a little degree of intelligence data that had indicated there were certain foreign nationals indulging in that type of flying lesson, it might have created a pattern of concern that would have possibly detected the advance notion of people plowing airplanes into tall buildings in our society.

I use that as an example, because it does seem to me there is an earlier reference to an intelligence breakdown. The use of vigilant intelligence and the need for both the horizontal and vertical communication of intelligence agencies in the United States is an absolute imperative at this time. And it's rather regrettable, I think, that we've been informed that the FBI and the CIA have not adequately communicated with one another, and certainly not adequately communicated with ***local*** law enforcement to promote vigilance at a time when it could be prudent.

We want to practice preventive medicine, essentially. I don't want to wait 'til the next thing happens and say, "It's a pity it happened. Let's do something about it now." I'd like to prevent it from occurring ever again. Because anyone who ***lives*** in New York will be forever scarred by what's just happened. And that's perhaps why I'm taking a fairly intense view of these discussions at this moment.

MS. SCHAKOWSKY: Thank you to all of you. I want to comment on this important discussion that we've been having. I think the example of flying lessons conducted by a company that gave them to what turned out to be a terrorist is an example of ways in which our current infrastructure failed us, and the ability to communicate information broke down. And we certainly are all interested in making sure that we fill in the cracks and make a seamless flow of information to the extent that we can.

But I have to say, Senator Goodman, that I too, feel that particularly at this time, when we're on a state of reflection about what is most precious about the United States, what are the things that are -- that make us meek and are so worth protecting, that we must proceed very cautiously, perhaps even more cautiously than when things are just

clicking along so smoothly. So that we don't make the kinds of overreaching mistakes that we did when we interned the Japanese.

And I know that you're certainly not talking about that kind of activity but I think that it is somewhat of a slippery slope and that we have to be very careful that we don't install permanent -- a reason, for example, that I voted "no" on a bill that I thought had many good provisions, the bill which I felt shouldn't have been called the Patriot Act, because I believe myself to be a patriot but voted "no" on that. So I think we have to be very, very careful as we proceed forward and I think that this conversation today and all of the witnesses, both panels, contributed to the kind of thoughtful debate that we need to have and I appreciate it very, very much.

REP. HORN: Well, I wanted particularly to appreciate what the ranking member did about the terrible breech of the constitution with the Japanese Americans ***going*** into internments. I'm proud to say my mother who was director of welfare in her county, she opened up and said that is just wrong and the person who -- the only person I know of who elected was against that, since Roosevelt and General De Witt just ***went*** ahead of everything with putting people in internment camps even ***going*** with the Army to Peru so forth. But the only elected person was a very interesting gentleman named Harry Cain, the Mayor of Tacoma, where many Japanese Americans were and he later was a United States senator and then President Eisenhower made him head of the subversive whatever board was in those days, and he had the guts to stand it. And I had lunch with the chief justice, Earl Warren, just before he died, about three months before, and that was, he felt, the biggest mistake he ever ***went*** and he was a wonderful man and very strong on civil liberties but one gets swept up in that and they do it, but it's wrong and we don't want to see that happen again.

So let me just ask one or two questions and we'll close it out. Mr. Ellison (sp) has offered to provide the databases for free for Oracle, does this include maintenance, technical support and upgrades? As long as you're in a Santa Claus mood, I just thought I'd --

MR. HOECHST: I would not venture to be able to speak for him on what's intended there. I would like to describe the nature of the intent of that offer which was to take advantage of the resources and the enthusiasm that commercial organizations like Oracle and others have to facilitate action and so Larry's comments, I believe, were to try and remove any roadblocks required to facilitate action toward building systems that can share information and if what we can do is provide free software or free maintenance on software or free services, can help a way to stimulate action rather than be roadblocks that cause processes to languish, then we'll do that.

REP. HORN: I have one question for Mrs. Corrigan. How would a consolidated identity system invade the privacy of individuals any more than the current systems: Social Security, drivers' license, passport, and we have that now.

MS. CORRIGAN: Well, actually we also have something called the Privacy Act which as I mentioned before is rooted in one basic principal and that is that information collected for one purpose, so whether it's either Museum of Modern Art in New York, or whether it's by the Social Security Administration, information collected for that purpose shouldn't be used for another purpose unless subject to one of the exceptions outlined in the law. And we at the SLU (?) are also very concerned about the misuse of such security numbers and privacy violations that ***go*** on every day.

But one of the biggest protections of privacy is actually the decentralized nature of the data, that it's one thing for my doctor to know my -- have access to my personal health information, it's another thing for law enforcement to have my arrest record, but it's a completely different thing for people to then combine those different pieces of information and come up and marry them and then come up with a whole profile of my ***life***. And as I mentioned before, you know, one accident in the federal government, unfortunately, has been subject to either accidents, in terms of security on the Web or, unfortunately, employees who are corrupt and sell or misuse that information. That, again, there's a difference when you have separate databases versus the marrying of the information, the privacy risk is just magnified.

REP. HORN: Well, I'll tell you, every hearing we've ever had on privacy in that is we wanted to make sure, and the speaker mentioned it this morning, you make a felony out of it. We had one of our colleagues when I came into the Congress, her medical file had been put in the papers, and why? A disgruntled employee or whatever, and that's why people have to be very careful of any files, in a doctor's office in particular.

DR. SHNEIDERMAN: I'd like to speak to that issue. There's a long history of the tension between centralized and decentralized systems and there are two issues. One is as Ms. Corrigan described, the centralized facility allows a single point of attack a single point of destruction, a single point of violation and, therefore, the magnitude of the violation is greater. The capacity of the computer to amplify our power to do good also amplifies the power to do evil, and therefore, someone can search across a much larger dataset in that way. But the other interesting point about the multiple, the diversified, decentralized approach actually it stimulates creative designs by having independent explorations and involves much more effective best practices if they then are shared and copied by the others, which is again why I encourage the collaboration by way of the National Association of State CIOs. So that the best practices of each of the 50 states could then be repeated and disseminated widely and that's truly one of the strengths of the decentralized approach.

REP. HORN: I'm ***going*** to thank the staff now and then have a closing bit of what I think this is ***going*** and the person on my left is the staff director and chief counsel for the subcommittee and Bonny Heald (sp) in back as the deputy staff director, Darren Chidsey (sp) is a professional staff member, Mark Johnson, our chief clerk, Earl Pearce, professional staff member, Jim Holmes (sp), intern, and then for the ranking member here, David Macmillan, professional staff member, and Jean Goesser (sp), minority clerk. Our court reporters, Laurie Shadakian (sp) and Nancy O'Rourke, and we thank you.

The hearing was not intended to resolve the national identification issue, but merely to advance the debate in light of September 11th attacks and the ***changed*** world in which we now ***live***. Our witnesses provided a variety of perspectives and brought a great deal of expertise to the discussion. We're only beginning to explore this complicated issue, but one thing is certain, the September 11th attacks as horrifying as they were have brought out the best in America. One small but important example of the nation's strength is the ability to conduct this calm, civil but vigorous discussion of whether America needs a national identification system and if so, how to ***go*** about creating it. Ultimately we can trust the American people and their representatives to make the right decision.

And with that we are adjourned.

END

Classification

Language: ENGLISH

Subject: TERRORISM (92%); SEPTEMBER 11 ATTACK (90%); NATIONAL IDENTITY CARDS (88%); TESTIMONY (78%); US DEMOCRATIC PARTY (78%); TERRORIST ATTACKS (77%); FRAUD & FINANCIAL CRIME (73%); NATIONAL SECURITY (72%); COUNTERTERRORISM (72%); CIVIL RIGHTS (64%); HOLDING COMPANIES (50%)

Company: ORACLE CORP (93%); ORACLE CORP (93%); AMERICAN CIVIL LIBERTIES UNION (84%); GEORGE WASHINGTON UNIVERSITY (84%); ASSOCIATION FOR COMPUTING MACHINERY (84%); UNIVERSITY OF MARYLAND (84%); ASSOCIATION FOR COMPUTING MACHINERY (84%); AMERICAN CIVIL LIBERTIES UNION (84%); GEORGE WASHINGTON UNIVERSITY (84%); UNIVERSITY OF MARYLAND (84%)

Organization: AMERICAN CIVIL LIBERTIES UNION (84%); GEORGE WASHINGTON UNIVERSITY (84%); ASSOCIATION FOR COMPUTING MACHINERY (84%); UNIVERSITY OF MARYLAND (84%); ASSOCIATION FOR COMPUTING MACHINERY (84%); AMERICAN CIVIL LIBERTIES UNION (84%); GEORGE WASHINGTON UNIVERSITY (84%); UNIVERSITY OF MARYLAND (84%)

Ticker: ORCL (NYSE) (93%)

Industry: AIRLINES (72%); AIRLINE EMPLOYEES (67%)

Person: JAN SCHAKOWSKY (59%)

Geographic: UNITED STATES (95%)

Load-Date: November 22, 2001
