TESTIMONY

Statement by J. Bradley Jansen,

Free Congress Foundation
A License to Break the Law?

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

Committee on Government Affairs
April 16, 2002

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

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

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

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

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

A national ID would depend on a massive bureaucracy that would limit our basic freedoms. A national ID system would depend on both the issuance of an ID card and the integration of huge amounts of personal information included in state and federal government databases. One employee mistake, an underlying database error rate, or

common fraud could take away an individual's ability to move freely from place to place or even make them unemployable until the government fixed their "file." Anyone who has attempted to fix errors in their credit report can imagine the difficulty of causing an over-extended government agency such as the department of motor vehicles to correct a mistake that precludes a person from getting a valid ID.

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

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

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

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

In addition to our concerns raised in that coalition letter, the Free Congress Foundation would like to stress that a proposal to standardize procedures is not a substitute for increasing standards. Richard Clarke, whom President Bush appointed last October as the chairman of the new Critical Infrastructure Protection Board, has been openly

dismissive of the alleged benefits of a National ID proposal and commented last year that he could not name one Bush official who supported the idea proposed by Oracle Chairman and CEO Larry Ellison[5]. Mr. Clarke has also been clear that more laws for improved computer security standards are unnecessary, "On the government systems side, we already have a lot of authority to issue standards and enforce them—we've never done that."[6]

The effect of standardizing procedures at a time of great technological change risks truncating the discovery process. The debate over biometric identifiers and the networking of databases only highlights that new capabilities from technological and other developments are constantly appearing. Adopting a single standard not only locks us in to a system that might or might not be the best system we could adopt now but it also locks us out of learning what applications of what new developments are best and should be more widely adopted.[7] Allowing the states to act as laboratories of democracy better assures us of the benefits of discovering the best applications of new technologies.

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

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

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

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

In conclusion, I applaud the subcommittee for taking an active role in such an important question. The development of new technologies, including biometrics, might be able to improve the quality of our identification systems but their capabilities should not be

exaggerated.[13] The focus of the federal government at this point should be to address the inadequacies of their own systems. Thank you again for this opportunity.

---

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

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

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

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

[5] Mills Abreau, Elinor, "Cyber-security czar snubs id plan, defends Govnet," Reuters, November 8, 2001.

[6] McCullagh, Declan, "The Sentinel," Wired magazine, p. 110, March 2002.

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

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

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

[10] "Use of stolen passport by highjackers: problems with Dept of State not keeping track," CNN.com, November 23, 2001. http://www.cnn.com/2001/US/11/23/inv.attacks.visas/index.html.

See also Schemo, Diana Jean and Robert Pear, "Loopholes in Immigration Policy Worked in Hijack Suspects' Favor," September 27, 2001. http://college4.nytimes.com/guests/articles/2001/09/27/870395.xml

[11] Phyllis Schafly, Eagle Forum letter to Representative Horn, November 15, 2001.

[12] Potter, Mark and Rich Phillips, CNN, "INS issuance of flight school visas to two terrorists recently: Six months after Sept. 11, hijackers' visa approval letters received," March 13, 2002. http://www.cnn.com/2002/US/03/12/inv.flight.school.visas/index.html.

[13] Cole, Simon, "The Myth of Fingerprints," The New York Times, May 13, 2001. http://www.truthinjustice.org/fingerprint-myth.htm.

Committee Members | Subcommittees | Hearings | Key Legislation | Jurisdiction
Press Statements | Current Issues | Video of Select Hearings | Sites of Interest