epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Prepared Testimony and Statement for the Record of

Melissa Ngo
Staff Counsel and Director of the Identification and Surveillance Project
Electronic Privacy Information Center

Hearing on

“Maryland Senate Joint Resolution 5”

Before the

Judicial Proceedings Committee
Maryland Senate

February 15, 2007
2 East Miller Senate Building
Annapolis, MD

Mr. Chairman, and members of the Committee, thank you for the invitation to appear before you today. My name is Melissa Ngo and I am Staff Counsel and Director of the Identification and Surveillance Project at the Electronic Privacy Information Center (EPIC) in Washington, DC. EPIC is a non-partisan public interest research organization established in 1994 to focus public attention on emerging civil liberties issues. We are very pleased that you have convened this hearing today on Senate Joint Resolution 5, "REAL ID Act of 2005 – Protest and Repeal."

EPIC has worked on identification issues, including the REAL ID Act, for many years.[1] We have testified about identification proposals before committees in the U.S. Senate and House on identification issues, and we have submitted comments on federal rulemakings concerning the subject. A month after the passage of the REAL ID Act, held a symposium on the Act and related proposals.[2] We also have written extensively about the REAL ID Act.[3]

In my statement today, I will summarize the problems with a national identification scheme, such as the one created by the REAL ID Act of 2005, including the privacy and security risks that are inherent in the system. The main point of my testimony today is to make clear the extraordinary impact that the REAL ID would have upon the state of Maryland and its residents if it is implemented. Congress rushed this proposal through without any hearings, debate, or even a vote. It is imperative that the Senate pass Joint Resolution 5.

The U.S. Congress Passed the REAL ID Without Debate

The REAL ID Act was appended to a bill providing tsunami relief and military appropriations, and passed with little debate and no hearings. It was passed in this manner even though Republican and Democratic lawmakers in the Senate urged Sen. Bill Frist to allow hearings on the bill and to permit a separate vote on the measure.[4] The senators said they believe REAL ID "places an unrealistic and unfunded burden on state governments and erodes Americans' civil liberties and privacy rights."[5]

[1] *See generally,* EPIC Page on National ID Cards, http://www.epic.org/privacy/id_cards/ and Privacy Int'l Page on National ID Cards, http://www.privacy.org/pi/issues/idcard/index.html (last visited Feb. 14, 2007).

[2] EPIC Page on June 6, 2005, National ID Symposium, http://www.epic.org/events/id/.

[3] *See* discussion *infra* of publications by Marc Rotenberg, EPIC Exec. Dir. and Bruce Schneier, security expert and member of the EPIC Bd. of Directors.

[4] Press Release, Senate Comm. on Homeland Sec. & Governmental Affairs, Twelve Senators Urge Frist To Keep Real Id Act Off Supplemental Appropriations Bill Sweeping Proposal Needs Deliberate Consideration (Apr. 12, 2005), *available at* http://www.senate.gov/%7Egov_affairs/index.cfm?FuseAction=PressReleases.Detail&Affiliation=R&PressRelease_id=953&Month=4&Year=2005.

[5] *Id.*

The REAL ID Act Creates a National Identification Card

The REAL ID Act of 2005 imposes federal technological standards and verification procedures on state driver's licenses and identification cards and mandates state compliance by May 2008, unless the Department of Homeland Security Secretary grants an extension.[6] REAL ID turns state DMV workers into federal immigration officials, as they must verify the citizenship status of all those who want a REAL ID-approved state driver's license or identification cards. State DMVs would far move away from their core mission -- to license drivers.

According to the federal legislation, state licenses and ID cards must meet standards set out in the REAL ID Act to be accepted for federal use, including entrance into a courthouse or onto a plane, and receiving federal benefits, such as Social Security or Medicare. The requirement for non-REAL ID driver's license or ID card to have explicit "invalid for federal purposes" designations turns this "voluntary" card into a mandatory national ID card. Anyone with a different license or ID card would be instantly suspicious. REAL ID cards will be necessary for federal purposes such as entering courthouses, air travel or receiving federal benefits, such as Medicaid or Social Security. It will be easy for insurance companies, credit card companies, even video stores, to demand a REAL ID driver's license or ID card in order to receive services. Significant delay, complication and possibly harassment or discrimination would fall upon those without a REAL ID card. The "voluntary" card, is in fact, a de facto mandatory national ID card.

Americans Have Rejected the Idea of a National Identification Card

When the Social Security Number (SSN) was created in 1936, it was meant to be used only as an account number associated with the administration of the Social Security system.[7] Though use of the SSN has expanded considerably, it is not a universal identifier and efforts to make it one have been consistently rejected. In 1973, the Health, Education and Welfare Secretary's Advisory Committee on Automated Personal Data Systems rejected the creation of a national identifier and advocated the establishment of significant safeguards to protect personal information. The committee said:

> We recommend against the adoption of any nationwide, standard, personal identification format, with or without the SSN, that would enhance the likelihood of arbitrary or uncontrolled linkage of records about people, particularly between government or government-supported automated personal data systems. What is needed is a halt to the drift toward [a standard universal identifier] and prompt action to establish safeguards

[6] Pub . L. No. 109-13, 119 Stat. 231 (2005).

[7] EPIC & PRIVACY INT'L, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND PRACTICE 47 (EPIC 2004).

> providing legal sanctions against abuses of automated personal data systems.[8]

In 1977, the Carter Administration reiterated that the SSN was not to become an identifier. In Congressional testimony in 1981, Attorney General William French Smith stated that the Reagan Administration was "explicitly opposed to the creation of a national identity card."[9] When it created the Department of Homeland Security, Congress made clear in the enabling legislation that the agency could not create a national ID system.[10] In September 2004, then-Department of Homeland Security Secretary Tom Ridge reiterated, "[t]he legislation that created the Department of Homeland Security was very specific on the question of a national ID card. They said there will be no national ID card."[11] The REAL ID Act creates a de facto national ID card, and Maryland should reject this imposition upon its residents.

The REAL ID Act Exacerbates the Identity Theft Problem

We have seen countless data breaches that have left the personal data of millions of Americans vulnerable to misuse. In February 2005, databroker Choicepoint sold the records of at least 145,000 Americans to a criminal ring engaged in identity theft obtained.[12] Also that year, Bank of America misplaced back-up tapes containing detailed financial information on 1.2 million employees in the federal government, including many members of Congress.[13] Last May, an information security breach by a Veterans Affairs employee resulted in the theft from his Maryland home of unencrypted data affecting 26.5 million veterans, active-duty personnel, and their family members.[14] The laptop and an external hard drive contained unencrypted information that included millions of Social Security numbers, disability ratings and other personal information.[15]

[8] Dep't of Health, Educ. & Welfare, Secretary's Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* (July 1973)*, available at* http://www.epic.org/privacy/hew1973report/.

[9] Robert B. Cullen, *Administration Announcing Plan*, Associated Press, July 30, 1981.

[10] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002),

[11] Tom Ridge, Sec'y, Dep't of Homeland Sec., *Address at the Center for Transatlantic Relations at Johns Hopkins University: "Transatlantic Homeland Security Conference"* (Sept. 13, 2004), *available at* http://www.dhs.gov/xnews/speeches/speech_0206.shtm (last visited Feb. 14, 2007).

[12] Robert O'Harrow Jr., *ID Theft Scam Hits D.C. Area Residents*, Wash. Post, Feb. 21, 2005, at A01; *see* EPIC's Page on ChoicePoint, http://www.epic.org/privacy/choicepoint/.

[13] Robert Lemos, *Bank of America loses a million customer records*, CNet News.com, Feb. 25, 2005.

[14] *See* EPIC's Page on the Veterans Affairs Data Theft, http://www.epic.org/privacy/vatheft/.

[15] Statement, Dep't of Veterans Affairs, A Statement from the Department of Veterans Affairs (May 22, 2006).

The REAL ID Act requires the collection of sensitive personal data yet lacks adequate privacy safeguards to protect the data. States are required to maintain paper copies or digital images of important identity documents, such as birth certificates or naturalized citizenship papers, for seven to 10 years, combined with the requirement to "provide electronic access to all other States to information contained in the motor vehicle database of the State" will make this data a tempting target for identity thieves. The 50 state (plus the District of Columbia) databases would become one large database. And one presumes that each DMV would have access to these databases at the very least to confirm that the applicant does not have a REAL ID license or ID card in another state. The theft of your REAL ID information would affect you more profoundly than the theft of you current license information. Anyone with access to your REAL ID data has access to your driver's license, your birth certificate, your Social Security Card, your marriage license – the list goes on. If a criminal could break the security of any one of the tens of thousands of entrance points, then the criminal would have access to the personal data, including Social Security numbers, of every single person in the United State with a REAL ID license or ID card. This would put hundreds of millions of people at risk for identity theft.

There is another significant security risk, besides that of attacks by unauthorized users, and that is of authorized users abusing their power. A 2005 scandal in Florida highlights risks associated with large databases, such as the one created by the REAL ID Act. A woman who wrote to a newspaper criticizing a Florida sheriff as being too fat for police work and his agency's use of stun guns.[16] Orange County Sheriff Kevin Beary ordered staffers to use state driver's license records to find the home address of his critic.[17] The sheriff sent her a letter at her home address, and she reported being surprised that he was able to track her down so easily.[18] In case in Maryland just last year, three people – including a Maryland Motor Vehicle Administration official – were indicted on charges of "conspiring to sell unlawfully produced MVA-issued Maryland identification cards."[19]

The consumer harm that results from the wrongful disclosure of personal information is very clear. According to the Federal Trade Commission, identity theft is the No. 1 crime in the country. For the seventh year in a row, identity theft topped the list of complaints, accounting for 36 percent of the 674,354 consumer fraud complaints filed with the agency last year.[20] Maryland was No. 11 in the rankings of identity theft victims by state, not a list Maryland wants to rank high on.[21] And there is every indication that

[16] *Called fat, sheriff tracks down reader*, Associated Press, Apr. 6, 2005.

[17] *Id*.

[18] *Id*.

[19] *Fake ID Cards*, Wash. Post, Mar. 15, 2006, at B02.

[20] Fed. Trade Comm'n, *Consumer Fraud and Identity Theft Compliant Data: January – December 2006* (Feb. 7, 2007), *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf (last visited Feb. 14, 2007).

[21] *Id.* at 18.

the level of this crime is increasing nationwide. The national identification database created by the REAL ID Act exacerbates the identity theft problem. By aggregating so much personal data in one place with many entry points, REAL ID creates a "one-stop shop" for identity thieves. Centralizing authority over personal identity into one database and one card increases both the risk of identity theft as well as the scope of harm when it occurs.

The Privacy and Security Issues of REAL ID Are Unresolved

In a recent analysis of the REAL ID Act, EPIC Executive Director Marc Rotenberg explained that "[s]ystems of identification remain central to many forms of security. But designing secure systems that do not introduce new risks is proving more difficult than many policymakers had imagined."[22] The biggest problem with the REAL ID Act is the failure to establish adequate privacy safeguards in a system to identify 245 million license and ID cardholders nationwide. Rotenberg explained that other countries are facing the same issues that the U.S. is now facing, and discussed the national ID debate in the United Kingdom. The U.K. government states that a national ID card will prevent crime and illegal immigration, among other things. But a report from the London School of Economics flatly rejected this notion, stating "ID requirements may actually make matters worse.[23] The report explained, "Even as cards are promised to be more secure, attacks become much more sophisticated. Most recently, Russian security agents arrested policemen and civilians suspected of forging Kremlin security passes that guaranteed entrance to President Vladimir Putin's offices."[24]

The theory that the REAL ID Act will prevent terrorism is predicated on the belief that only "outsiders" have an intent to harm the United States. Bruce Schneier, security expert and member of the EPIC Board of Directors, has explained the misconception thusly, "In theory, if we know who you are, and if we have enough information about you, we can somehow predict whether you're likely to be an evildoer."[25] This is impossible, because you cannot predict intent based on identification, Schneier said.[26]

[22] Marc Rotenberg, EPIC Exec. Dir., *Real ID, Real Trouble?*, COMMUNICATIONS OF THE ACM, Mar. 2006, *available at* http://www.epic.org/privacy/id_cards/mr_cacm0306.pdf.

[23] London School of Economics, Dep't of Info. Systems, *The Identity Project: an assessment of the UK Identity Cards bill and its implications* (June 2005), *available at* http://is.lse.ac.uk/idcard/identityreport.pdf (last visited Feb. 14, 2007); London School of Economics*, Research Status Report*, pp. 7, 10 (Jan. 2006) *available at* http://is.lse.ac.uk/idcard/statusreport.pdf (last visited Feb. 14, 2007).

[24] *Id*.

[25] Bruce Schneier, *Real-ID: Costs and Benefits,* BULLETIN OF ATOMIC SCIENTISTS, Mar./Apr. 2007, *available at* http://www.schneier.com/blog/archives/2007/01/realid_costs_an.html (last visited Feb. 14, 2007).

[26] *Id*.

But, as with databases, there are threats from both sides. Terrorist acts have been committed by U.S. citizens, "insiders." Oklahoma City bombers Timothy McVeigh and Terry Nichols were U.S. citizens. As was Unabomber Ted Kaczynski.

There is also the threat that REAL ID is ostensibly trying to protect against: forged identification cards. "No matter how unforgeable we make it, it will be forged. We can raise the price of forgery, but we can't make it impossible. Real IDs will be forged," Schneier said.[27] This means that people with evil intent will get legitimate REAL ID cards in fake names, or even in the names of read people whose identities have been stolen, he said.[28]

The REAL ID Act Could Harm Maryland's Domestic Violence Victims

The REAL ID Act threatens Maryland's address confidentiality program, and this threat has the potential to harm Maryland's domestic violence victims. The Maryland Safe At Home program allows victims of domestic violence to use a substitute address when interacting with the state.[29] Victims register with the state, and the program forwards mail received at the substitute address while keeping the actual residential address confidential. A participant in the Safe At Home program can request that the Maryland Motor Vehicle Administration use the substitute address, thereby allowing the domestic violence victim to keep her residential address off driver's license and vehicle registration lists, among others.[30] Having the substitute address on her state identification card also aids the victim in using the substitute address with private sector organizations, such as a bank, allowing her to maintain the confidentiality of her residential address.

The REAL ID Act requirement that state driver's licenses and identification cards must list a person's actual address is a grave threat to this program.[31] Including data collection requirements without adequate privacy safeguards would put these victims at risk. The state of Maryland should not make it more difficult for a domestic abuse victim to hide from her abuser. Though the 2005 reauthorization of the Violence Against Women Act requested that the Department of Homeland Security "consider the needs" of people in confidentiality programs,[32] there is no guarantee that the Safe At Home program will be able to continue if Maryland implements the REAL ID Act.

The REAL ID Act Will Cause Significant Delays for Maryland Residents

Under the REAL ID Act, the Maryland Motor Vehicle Administration must verify a cardholder's name, date of birth, Social Security number, place of residence and

[27] *Id.*

[28] *Id.*

[29] Maryland Safe At Home Address Confidentiality Program, Questions and Answers, http://www.sos.state.md.us/ACP/QandA.pdf (last visited Feb. 14, 2007).

[30] MD. CODE REGS. 01.02.11.04 (2007).

[31] Pub. L. No. 109-13, § 202(b)(6), 119 Stat. 231, 312 (2005).

[32] Pub. L. No. 109-162, § 827, 119 Stat. 2960, 3066 (2005).

citizenship status, "with the issuing agency." This creates an incredible bureaucracy. All state MVAs would have to have secure access to state and federal databases with this information. These databases have been found to have inaccurate or incomplete information, which would significantly affect applicants.

Various reports have found errors in Social Security, employment, watch list and other government databases. For example, last month, the head of Transportation Security Administration said that the terror watch lists were being reviewed for errors, and he expected to cut the list of names, estimated at 325,000, in half.[33]

Imagine the delays, as state DMV workers will be forced to become federal immigration officers, verifying the birth and citizenship status of applicants. What happens to those whose birth certificates were lost through natural disaster – when a fire or a hurricane wipes out entire towns, and their data is lost?

The REAL ID Act Will Cost Maryland Residents Millions

Although the Congressional Budget Office has estimated the cost of implementing the Act to be around $100 million, the National Conference of State Legislatures has released a report estimating the cost to be $11 billion over the first five years.[34] This $11 billion includes estimates for re-enrollment of current cardholders, new verification process, new card design requirements, and support costs. So far, Congress has only appropriated $40 million total for the states to implement REAL ID. The states will have to look elsewhere for the other $10.96 billion needed. It is likely that state residents will bear the burden of paying for this national identification scheme.

Senate Joint Resolution 5 Will Reject National Identification Program

The bill under consideration today will do the following: refuse to implement the REAL ID Act, protest the actions of the Congress and the President in passing and signing the legislation, requests the repeal of REAL ID, and notify the Maryland Congressional delegation, governor, president of Senate of Maryland, and speaker of the

[33] *Hearing on Aviation Security: Reviewing the Recommendations of the 9/11 Commission Before the S. Comm. on Commerce, Science & Transp.*, 110th Cong. (Jan. 17, 2007) (Testimony of Edmund S. "Kip" Hawley, Assistant Sec'y, Transp. Sec. Admin., Dep't of Homeland Sec., *available at* http://commerce.senate.gov/public/_files/TestimonyofMrHawley.pdf (last visited Feb. 14, 2007).

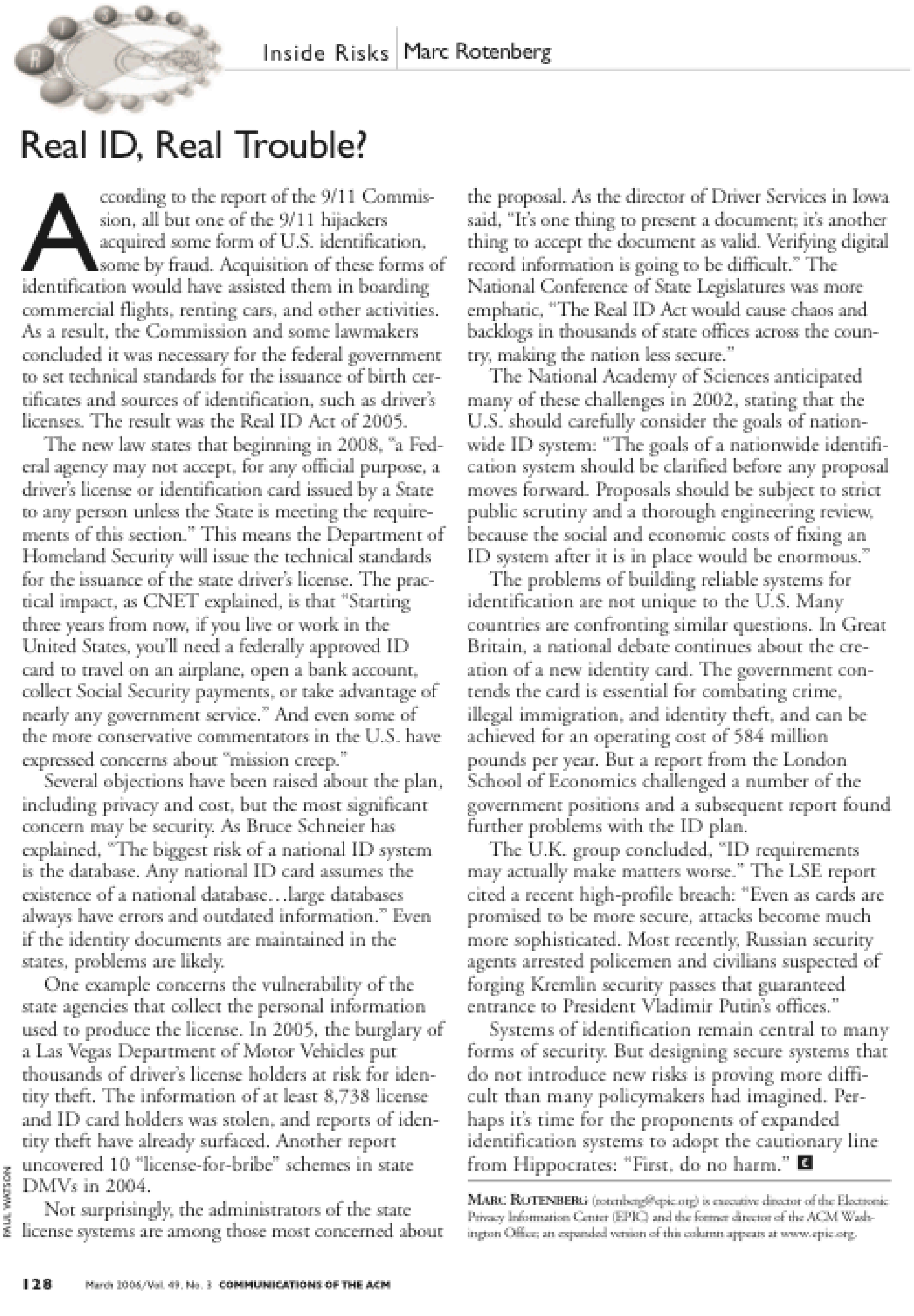
[34] Cong. Budget Office, *Cost Estimate: H.R. 418: REAL ID Act of 2005* (Feb. 9, 2005), *available at* http://www.cbo.gov/showdoc.cfm?index=6072&sequence=0&from=6 (last visited Feb. 14, 2007); Nat'l Conference of State Legislatures, *The REAL ID Act: National Impact Analysis* (Sept. 19, 2006), *available at* http://www.ncsl.org/print/statefed/Real_ID_Impact_Report_FINAL_Sept19.pdf (last visited Feb. 14, 2007).

House of Delegates of the resolution. This is a sensible response by Maryland to an ill-conceived federal law.

Conclusion

Nationwide, 245 million people have state driver's licenses or identification cards, and they will all be affected if REAL ID is implemented by the states. Last month, the state of Maine rejected the REAL ID Act. Maine passed a resolution stating that the "Maine State Legislature refuses to implement the REAL ID Act and thereby protest the treatment by Congress and the President of the states as agents of the federal government."[35] In passing Senate Joint Resolution 5, "REAL ID Act of 2005 – Protest and Repeal," Maryland will reject the national identification card that has so many costs to its residents. I appreciate the opportunity to be here today. I will be pleased to answer your questions.

[35] S.P. 113, 123d Leg., 1st Reg. Sess. (Me. 2007).



Real ID, Real Trouble?

According to the report of the 9/11 Commission, all but one of the 9/11 hijackers acquired some form of U.S. identification, some by fraud. Acquisition of these forms of identification would have assisted them in boarding commercial flights, renting cars, and other activities. As a result, the Commission and some lawmakers concluded it was necessary for the federal government to set technical standards for the issuance of birth certificates and sources of identification, such as driver's licenses. The result was the Real ID Act of 2005.

The new law states that beginning in 2008, "a Federal agency may not accept, for any official purpose, a driver's license or identification card issued by a State to any person unless the State is meeting the requirements of this section." This means the Department of Homeland Security will issue the technical standards for the issuance of the state driver's license. The practical impact, as CNET explained, is that "Starting three years from now, if you live or work in the United States, you'll need a federally approved ID card to travel on an airplane, open a bank account, collect Social Security payments, or take advantage of nearly any government service." And even some of the more conservative commentators in the U.S. have expressed concerns about "mission creep."

Several objections have been raised about the plan, including privacy and cost, but the most significant concern may be security. As Bruce Schneier has explained, "The biggest risk of a national ID system is the database. Any national ID card assumes the existence of a national database…large databases always have errors and outdated information." Even if the identity documents are maintained in the states, problems are likely.

One example concerns the vulnerability of the state agencies that collect the personal information used to produce the license. In 2005, the burglary of a Las Vegas Department of Motor Vehicles put thousands of driver's license holders at risk for identity theft. The information of at least 8,738 license and ID card holders was stolen, and reports of identity theft have already surfaced. Another report uncovered 10 "license-for-bribe" schemes in state DMVs in 2004.

Not surprisingly, the administrators of the state license systems are among those most concerned about the proposal. As the director of Driver Services in Iowa said, "It's one thing to present a document; it's another thing to accept the document as valid. Verifying digital record information is going to be difficult." The National Conference of State Legislatures was more emphatic, "The Real ID Act would cause chaos and backlogs in thousands of state offices across the country, making the nation less secure."

The National Academy of Sciences anticipated many of these challenges in 2002, stating that the U.S. should carefully consider the goals of nationwide ID system: "The goals of a nationwide identification system should be clarified before any proposal moves forward. Proposals should be subject to strict public scrutiny and a thorough engineering review, because the social and economic costs of fixing an ID system after it is in place would be enormous."

The problems of building reliable systems for identification are not unique to the U.S. Many countries are confronting similar questions. In Great Britain, a national debate continues about the creation of a new identity card. The government contends the card is essential for combating crime, illegal immigration, and identity theft, and can be achieved for an operating cost of 584 million pounds per year. But a report from the London School of Economics challenged a number of the government positions and a subsequent report found further problems with the ID plan.

The U.K. group concluded, "ID requirements may actually make matters worse." The LSE report cited a recent high-profile breach: "Even as cards are promised to be more secure, attacks become much more sophisticated. Most recently, Russian security agents arrested policemen and civilians suspected of forging Kremlin security passes that guaranteed entrance to President Vladimir Putin's offices."

Systems of identification remain central to many forms of security. But designing secure systems that do not introduce new risks is proving more difficult than many policymakers had imagined. Perhaps it's time for the proponents of expanded identification systems to adopt the cautionary line from Hippocrates: "First, do no harm." ■

MARC ROTENBERG (rotenberg@epic.org) is executive director of the Electronic Privacy Information Center (EPIC) and the former director of the ACM Washington Office; an expanded version of this column appears at www.epic.org.

PAUL WATSON