Prepared Testimony and Statement for the Record of

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

Meeting on

"REAL ID Rulemaking"

Before the

Data Privacy and Integrity Advisory Committee
Department of Homeland Security

March 21, 2007
Crowne Plaza Washington National Airport
Arlington, VA

Members of the Committee, thank you for the invitation to appear before you today. My name is Melissa Ngo and I am Director of the Identification and Surveillance Project at the Electronic Privacy Information Center (EPIC) in Washington, D.C. EPIC is a non-partisan public interest research organization established in 1994 to focus public attention on emerging civil liberties issues. We are pleased that you have convened this meeting today on "REAL ID Rulemaking."

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, 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] We have written an in-depth analysis of the proposed Department of Homeland Security ("DHS") regulations to implement REAL ID and will be submitting comments to the agency about the rulemaking.[4]

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 and the proposed DHS regulations. The main point of my testimony today is to make clear that the Department of Homeland Security's proposed regulations do not solve the fundamental threats to national security and individual privacy created by this national identification scheme. The biggest problem is the failure to establish adequate privacy and security safeguards in a system to identify 245 million license and ID cardholders nationwide.

The REAL ID Act and Proposed Regulations Create a National Identification System

The REAL ID Act of 2005 imposes federal technological standards and verification procedures on state driver's licenses and identification cards.[5] 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 move far away from their core mission -- to license drivers.

State licenses and identification cards must meet standards set out in the regulations to be accepted for federal use. Such federal purposes include entering buildings, boarding commercial aircraft, entering nuclear power plants, and "any other purposes that the Secretary shall determine."[6] DHS may compel card design

---

[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 Mar. 19, 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 EPIC Bd. of Directors.
[4] EPIC, Spotlight on Surveillance, *Federal REAL ID Proposal Threatens Privacy and Security* (Mar. 2007), http://www.epic.org/privacy/surveillance/spotlight/0307.
[5] Pub. L. No. 109-13, 119 Stat. 231 (2005).
[6] Dep't of Homeland Sec., *Notice of proposed rulemaking: Minimum Standards for Driver's licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes,* 72 Fed. Reg. 10,819 (Mar. 9,

standardization, "whether a uniform design/color should be implemented nationwide for non-REAL ID driver's licenses and identification cards," so that non-REAL ID cards will be easy to spot.[7] This universal card design, combined with the mandate under the proposed regulations imposing new requirements on state motor vehicle agencies so that the federal government can link together their databases to distribute license and cardholders' personal data, create a national identification card.[8] "DHS is committed to the expedited development and deployment of a common [federated] querying service to facilitate the State DMV queries for REAL ID data verification," according to the regulations.[9]

REAL ID Creates Significant Threats to National Security and Individual Privacy

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."[10] 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."[11] This is impossible, because you cannot predict intent based on identification, Schneier said.[12] 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.[13] Upon the release of the draft regulations, Schneier said, "The REAL ID regulations do not solve problems of the national ID card, which will fail when used by

---

2007) [hereinafter "REAL ID Draft Regulations"], *available at* http://a257.g.akamaitech.net/7/257/2422/01jan20071800/edocket.access.gpo.gov/2007/07-1009.htm (last visited Mar. 19, 2007).

[7] *Id*. at 10,841.

[8] *Id*. at 10,825.

[9] *Id*.

[10] 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.

[11] 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 Mar. 19, 2007).

[12] *Id*.

[13] *Id*.

someone intent on subverting that system. Evildoers will be able steal the identity -- and profile -- of an honest person, doing an end-run around the REAL ID system."[14]

A recent case illustrates Schneier's point. According to court documents, a few weeks ago in Florida, two men entered restricted areas, bypassed security screeners and carried a duffel bag containing 14 guns and drugs onto a commercial plane."[15] They avoided detection, because they are airline baggage handlers who used their uniforms and legally issued identification cards.[16] Both men had passed federal background checks before they were hired, according to a spokesman for Comair, the airline that employed the men.[17] The men were only investigated and caught after receiving an anonymous tip.[18] If the airport had identification-neutral security systems, such as requiring all fliers go through metal detectors, then the men could not have walked past them. But the identification-based security system – allowing some fliers to skip screening because they are presumed to have no evil intent – failed, and the men transported weapons and contraband aboard a commercial flight.

The DHS Regulations Do Not Resolve the Fundamental Problems in REAL ID

The Department of Homeland Security regulations for Real ID dictate the expansion of schedules and procedures for retention and distribution of identification documents and other personal data. The regulations create a massive database with the personal data and copies of identification documents of 245 million state license and identification cardholders nationwide. Yet DHS has chosen not to mandate minimum privacy standards for either the database or the card itself.

On security and privacy standards for the system, state motor vehicle facilities, and the personal data and documents collected in state motor vehicle databases, DHS proposes that states prepare a "comprehensive security plan" for REAL ID implementation.[19] The vague plan proposes that states would include 1) an "approach to conducting background checks of certain federal employees"; 2) an approach to ensuring the "physical security of the locations where driver's licenses and identification cards are produced"; 3) an approach to ensuring the "security of document materials and papers from which driver's licenses and identification cards are produced"; 4) a description of the "security features incorporated into the driver's licenses and identification cards"; and 5) if the state decides to use biometrics as a part of its security plan, the state must "describe this use in its security plan and present the technology standard the State intends to use to DHS for approval."[20]

---

[14] Press Release, EPIC, After Long Delay, Homeland Security Department Issues Regulations For Flawed National ID Plan (Mar. 2, 2007) [hereinafter "EPIC Press Release on Regulations"], *available a*t http://www.epic.org/press/030207.html.
[15] Jim Ellis, *Feds: Bag Of Guns Smuggled Onto Plane*, Associated Press, Mar. 9, 2007.
[16] *Id*.
[17] *Id*.
[18] *Id*.
[19] REAL ID Draft Regulations at 10,822, *supra* note 6.
[20] *Id*. at 10,839-840.

DHS sets out standards for background checks on employees and for the type of paper the identification cards will use, yet it does not mandate any minimum standards of security for the national database of sensitive personal information. State DMVs already are the victims of outside attackers and insider license-for-bribe schemes. Even though standards for employee background checks are set out, this does not solve the "insider attack" problem, because there are insiders without previous ties to criminal activity. For example, the airport baggage handlers who were able to circumvent airport security and bring guns and drugs onto a commercial flight in Florida had passed federal background checks.

The creation of this massive database comes at a time when security breaches and identity theft are on the rise. For the seventh year in a row, identity theft is the No. 1 concern of U.S. consumers, according to the Federal Trade Commission's annual report.[21] Over 104 million data records of U.S. residents have been exposed due to security breaches since January 2005, according to a report from the Privacy Rights Clearinghouse.[22]

Under the required changes to the design of state licenses and identification cards, DHS states the card must include "[p]hysical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purpose" and "common [machine-readable technology], with defined minimum data elements."[23] The federal agency will require the use of a two-dimensional bar code, but will not require the use of encryption. Though Homeland Security lays out the privacy and security problems associated with creating an unencrypted machine readable zone on the license, it does not require encryption because there are concerns about "operational complexity."[24]

The Department of Homeland Security's own Privacy Office has urged the use of encryption in REAL ID cards. In its Privacy Impact Assessment of the draft regulations, the Privacy Office supported encryption "because 2D bar code readers are extremely common, the data could be captured from the driver's licenses and identification cards and accessed by unauthorized third parties by simply reading the 2D bar code on the credential" if the data is left unencrypted.[25] DHS says that, "while cognizant of this problem, DHS believes that it would be outside its authority to address this issue within this rulemaking."[26] Imposing a requirement for the states to use unencrypted machine readable technology renders the cardholder unable to control who receives her data.

---

[21] 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 Mar. 19, 2007).
[22] Privacy Rights Clearinghouse, Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Mar. 19, 2007).
[23] REAL ID Draft Regulations at 10,835, *supra* note 6.
[24] *Id*. at 10,826.
[25] Dep't of Homeland Sec. Privacy Office, *Privacy Impact Assessment for the REAL ID Act* 16 (Mar. 1, 2007), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realid.pdf (last visited Mar. 19, 2007) *and* http://www.epic.org/privacy/id_cards/pia_030107.pdf.
[26] REAL ID Draft Regulations at 10,837, *supra* note 6.

Third parties such as insurance companies are not the only ones who will try to broaden the use of the REAL ID card. State licenses and identification cards must meet standards set out in the regulations to be accepted for federal use. Such federal purposes include entering buildings, boarding commercial aircraft, entering nuclear power plants, and "any other purposes that the Secretary shall determine." The Department of Homeland Security, via the draft regulations and Homeland Security Secretary Michael Chertoff, discusses expanding the use of the national identification card. The federal agency seeks comments on "how DHS could expand [the card's official purposes] to other federal activities."[27] In a speech last month, Secretary Chertoff said the REAL ID Act licenses might "do double-duty or triple-duty."[28] These REAL ID cards would "be used for a whole host of other purposes where you now have to carry different identification."[29]

In his book, "Identity Crisis: How Identification is Overused and Misunderstood," Jim Harper, Director of Information Policy Studies at the Cato Institute, that the REAL ID Act and the regulations do not add to the nation's security protections.[30] Harper advocates a diverse identification system. "A diverse, competitive identification and credentialing industry would be far better, and far more protective of liberty, than the uniform government-monopolized identification system on the advance today."[31]

Security expert Bruce Schneier, EPIC and others have explained that it decreases security to have one ID card for many purposes, as there will be a substantial amount of harm when the card is compromised.[32] Using a national ID card would be as if you used one key to open your house, your car, your safe deposit box, your office, and more. "The problem is that security doesn't come through identification; security comes through measures -- airport screening, walls and door locks -- that work without relying on identification," therefore a national identification card would not increase national security Schneier said.[33]

Conclusion

The Department of Homeland Security regulations for Real ID would (1) impose more difficult standards for acceptable identification documents that could limit the ability of individuals to get a state driver's license; (2) compel data verification

---

[27] *Id*. at 10,823.
[28] Michael Chertoff, Sec'y, Dep't of Homeland Sec., *Remarks by Secretary Michael Chertoff at the National Emergency Management Association Mid-Year Conference* (Feb. 12, 2007), *available at* http://www.dhs.gov/xnews/speeches/sp_1171376113152.shtm (last visited Mar. 19, 2007).
[29] *Id*.
[30] JIM HARPER, IDENTITY CRISIS: HOW IDENTIFICATION IS OVERUSED AND MISUNDERSTOOD (Cato Institute 2006).
[31] *Id*. at 5.
[32] Melissa Ngo, Dir., EPIC Identification & Surveillance Project, *Prepared Testimony and Statement for the Record at a Hearing on "Maryland Senate Joint Resolution 5" Before the Judicial Proceedings Comm. of the Maryland Senate* (Feb. 15, 2007), *available at* http://www.epic.org/privacy/id_cards/ngo_test_021507.pdf.
[33] EPIC Press Release on Regulations, *supra* note 14.

procedures that the federal government itself is not capable of following; (3) mandate minimum data elements required on the face of and in the machine readable zone of the card; (4) require changes to the design of licenses and identification cards (5) expand schedules and procedures for retention and distribution of identification documents and other personal data; and (6) dictate state collection of personal data and documents without setting adequate security standards for the card, state motor vehicle facilities, or state motor vehicle databases. Most importantly, the REAL ID Act and the DHS regulations create a national identification system.

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. Legislation to repeal REAL ID has been introduced in the House and Senate. Maine and Idaho have passed resolutions rejecting implementation of REAL ID, and 25 other states are debating similar legislation. The Data Privacy and Integrity Advisory Committee should use its authority to advise the Department of Homeland Security that the proposed regulations do not solve the fundamental problems inherent in this national identification scheme. Only repeal of REAL ID will solve the problems created by this ill-conceived federal law.

I appreciate the opportunity to be here today. I will be pleased to answer your questions.

Attachment:

EPIC, Spotlight on Surveillance, *Federal REAL ID Proposal Threatens Privacy and Security* (Mar. 2007).