Testimony of Ari Schwartz
Vice President
Center for Democracy & Technology

Before the U.S. Senate Committee on Homeland Security and Governmental Affairs

Hearing on "Identification Security: Reevaluating the REAL ID Act"

July 15, 2009

On behalf of the Center for Democracy and Technology (CDT), thank you for the opportunity to participate in this hearing on Identification Security and S. 1261, the PASS ID Act.

CDT is a nonprofit, public interest organization dedicated to keeping the Internet open, innovative and free. CDT has been a leader in the policy debates over privacy issues raised by government identification programs. In particular, CDT has argued that Congress should amend the REAL ID Act to address key privacy flaws in the program and promote stronger privacy protections in state ID initiatives that threaten privacy and security separate and apart from the mandates of REAL ID.

CDT applauds the Committee for revisiting the REAL ID Act and commends Senators Akaka and Voinovich for initiating a dialogue on how identification security can be improved in a privacy-protective way. Our testimony will begin with some observations about the privacy issues associated with government identification programs and will describe how REAL ID exacerbated these privacy concerns. We will then offer CDT's analysis of the PASS ID Act. We will close with some suggestions for how Congress might strengthen the bill.

CDT has long supported the goal of making driver's license issuance more secure. The 9/11 Commission drew attention to crucial security gaps associated with the issuance of driver's licenses and ID cards. However, starting even before 9/11, but spurred by these findings, states have been moving towards greater standardization of driver's license design and greater centralization of personal data in Department of Motor Vehicle (DMV) databases, and those efforts will likely continue regardless of what Congress does. Three key trends in state driver's license programs pose serious privacy concerns for the 240 million Americans and lawful residents who carry government-issued identification credentials:

1) Driver's licenses and ID cards are being designed with standardized machine-readable zones (MRZs), and these features are being implemented in unprotected and interoperable ways.

2) Because information contained on cards is unprotected and the technologies are interoperable, information in the MRZ can be read, stored, and re-used by commercial and governmental entities with few limitations, facilitating intrusive tracking and profiling.

3) ID card systems increasingly include a centralized back-end information component containing vast amounts of identity data, vulnerable to theft and internal abuse if not properly protected.

REAL ID failed to address the concerns raised by these trends. In fact, the Act and final rule created new privacy and security risks while exacerbating old ones. If REAL ID were to go forward, it would:

- Create a *de facto* national ID system with a serious risk of mission creep. If fully implemented, the program presents the very real possibility that individuals would not be able to function in American society without a REAL ID card.

- Centralize vast amounts of sensitive, personally identifiable information (PII) through the creation of a centralized ID database. Such a database would create a valuable treasure trove of identity data, vulnerable to identity thieves, hackers, and internal abuse.

- Mandate a standardized MRZ on all REAL ID cards without requiring protections against skimming, which will facilitate intrusive tracking by unauthorized governmental and private entities.

- Fail to adopt meaningful privacy and security standards for the protection of personal information in the REAL ID system.

The REAL ID Act is not the only troublesome ID card program. In a related initiative, the Department of Homeland Security (DHS) is creating enhanced driver's licenses with imbedded, insecure RFID chips (so-called "vicinity-read" RFID) that will threaten the personal privacy and security of many American citizens living and working along our borders. The State Department's passport card also incorporates these insecure RFID chips.

The approach proposed in the PASS ID Act, S. 1261, mitigates many of the major privacy risks that REAL ID created while still imposing minimum standards for driver's license issuance. Most notably, the PASS ID Act:

- Eliminates the requirement under REAL ID that states give all other states "electronic access" to personal information in DMV databases, thus taking away one impetus for further centralization of identity data.

- Removes from DHS's authority the ability to unilaterally determine new official purposes for which a PASS ID-compliant card can be required, mitigating (though not eliminating) the potential for mission creep.

- Requires that states adopt privacy and security safeguards for personally identifiable information contained in DMV databases.

- Provides some protections for personal information stored in the MRZ by limiting the storage, use, and re-disclosure of that information by unauthorized third parties.

The new bill incorporates nearly all of the substantial privacy protections from the REAL ID repeal bill that CDT supported in front of this committee in the 110th Congress and a few more. CDT urges Congress to ensure that these provisions are not weakened.

While PASS ID is a major improvement over current law, the bill should be strengthened to further protect privacy and civil liberties while still achieving security objectives. PASS ID provides the opportunity to establish privacy guidance and protections for features of the state driver's license system that will exist regardless of REAL ID. Specifically, PASS ID could be further strengthened by:

- Mandating encryption or other security features to protect against unauthorized scanning of information in the licenses' MRZ.

- Limiting the data elements that may be contained on the MRZ to only what is necessary for legitimate law enforcement or DMV administrative purposes. (This could be accomplished by amending § 242(b)(9) in the proposed Title II, Subtitle E of the Homeland Security Act.)

- Reject the use of "vicinity-read" RIFD technologies (now incorporated in enhanced driver's licenses) in PASS ID cards. (This could be accomplished by amending § 242(a)(4) in the proposed Title II, Subtitle E of the Homeland Security Act.)

- Require encryption to protect any PII transmitted electronically for PASS ID compliance purposes. (This could be achieved in Sec. 5(b)(2) of the PASS ID Act.)

- Remove or substantially shorten the retention requirement for physical or electronic copies of source documents. (This could be addressed in § 242(d)(1) in the proposed Title II, Subtitle E of the Homeland Security Act.)

CDT looks forward to working with Congress to make these and other improvements to the PASS ID Act as the bill moves forward.

Government Identification Programs Raise Privacy Concerns

In recent years, the federal government has launched a variety of ID card programs, with the goal of making government-issued cards more reliable as identity credentials and to address the security gaps identified by the 9/11 Commission. Alongside these initiatives, states have been redesigning their driver's license systems to incorporate a number of advanced technology features.

While the goal of increasing security in the issuance of driver's licenses and ID cards is an important one, it should not be pursued without addressing the critical privacy and security risks posed by the technology features and back-end information systems that these ID programs are beginning to incorporate. Three key trends in ID card development threaten the civil liberties of the 240 million Americans and lawful residents who hold government-issued identity credentials:

1) Driver's licenses and ID cards are being designed with standardized machine-readable zones (MRZs), and these features are being implemented in unprotected and interoperable ways;

2) Because the information on the cards is not protected against skimming and the technologies are interoperable, the cards can be read by unauthorized commercial and governmental entities and the electronic data they contain can be stored and redisclosed, facilitating intrusive tracking and profiling; and

3) ID card systems increasingly include a centralized back-end information component containing vast amounts of sensitive, personally identifiable information (PII), which attracts motivated hackers and identity thieves and facilitates internal abuse if not properly protected.

The irony is that many technologies aimed at providing more secure licenses or more efficient licensing can actually threaten both security and privacy if not properly designed and implemented. CDT has reported on examples of these cases in the past and it is important to recognize that these threats to individual Americans continue to occur frequently.[1] Many recent cases of internal abuse and data theft underscore yet again the need for minimum standards to protect against unauthorized use and disclosure of sensitive PII collected and maintained at state DMVs:

- North Carolina -- Thieves stole a computer containing records from a DMV office, including Social Security numbers, birth dates, and driver's license numbers. The DMV believes that the theft's purpose was to make counterfeit licenses. The DMV took three weeks to notify the 16,000 people affected by the breach.[2]

- California -- Five former DMV employees were found guilty in a fake ID scheme, issuing fraudulent driver's licenses and identification cards between November 2003 and July 2005 for bribes. People paid $1,000 to $1,500 per license.[3]

- Colorado -- Security flaws were found that could affect all 3.4 million active DMV records. The State Auditor discovered that the DMV "sends large batches of personal information over the Internet without encryption" (in clear text). In addition, the DMV did not reset database permissions properly, and up to 33 former employees were still able to access the Driver's License Information System database (some for over one year after their departure). Accessible information included names, addresses, dates of birth, and Social Security numbers.[4]

---

1 Center for Democracy & Technology, "Unlicensed Fraud: How bribery and lax security at state motor vehicle offices nationwide lead to identity theft and illegal driver's licenses" (January 2004), available at http://www.cdt.org/privacy/20040200dmv.pdf.

2 Associated Press, "Thieves take N.C. DMV computer with personal info," WCNC, September 28, 2006.

3 Henry K. Lee, "Former DMV worker sentenced to 366 days in ID scam," San Francisco Chronicle, April 30, 2007.

4 Jessica Fender, "DMV puts Coloradans at risk of ID theft," Denver Post, July 9, 2008.

- Washington, D.C. -- A former DMV employee was found guilty of issuing around 200 licenses to individuals who did not live in the district or were not U.S. citizens. People were charged $1,000 to $1,700 per license.[5]

- Massachusetts -- A Registry of Motor Vehicles employee was arrested for issuing driver's licenses to undocumented workers for $1,000 each. The employee is accused of creating licenses with Social Security cards and birth certificates that belonged to people other than the ones she issued licenses to.[6]

These incidents make it clear that the computerization and centralization of driver's license data creates risks to both security and privacy. The addition to cards of advanced features such as an MRZ does not necessarily produce more secure or reliable cards, especially if the back-end databases and other procedures are insecure. Congress should be concerned about these types of incidents, not only for national security purposes but also because such abuses place everyday Americans at increased risk of identity theft and intrusive tracking by third parties. These incidents demonstrate the need for stronger minimum standards for card issuance and privacy protections for associated identity information to ensure that privacy and security risks are not aggravated in the process of trying to improve driver's license and ID card issuance.

REAL ID and Related Initiatives Exacerbate Privacy and Security Risks

REAL ID (as defined by the REAL ID Act and DHS's final rule) and the related enhanced driver's license (EDL) and passport card initiatives exemplify problematic trends in government identity programs. In fact, these programs have been implemented in a way that exacerbates the privacy and security concerns, defeating many of their professed security objectives.

REAL ID

Following the 2001 terrorist attacks, the 9/11 Commission Report underscored the need for minimum federal standards for issuance of driver's licenses and ID

5 Timothy Warren, "DMV worker gets time in prison; Paid to issue fake licenses," Washington Times, August 15, 2008.

6 Eric Moskowitz, "Registry worker charged in bribe licensing scheme," Boston Globe, March 20, 2009.

cards. To implement the Commission's recommendation, the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 established a negotiated rulemaking process to craft such standards. However, before that process could bear fruit, Congress passed the REAL ID Act of 2005. Added as a rider to a war and tsunami relief appropriations bill, the REAL ID Act was passed with little debate or input from key stakeholders, including privacy advocates.

More importantly, the REAL ID approach presented critical privacy and security risks. If implemented, the REAL ID Act would:[7]

- **Create a *de facto* national ID system with a serious risk of mission creep**: The REAL ID Act and final rule would create a *de facto* national ID system for the 240 million Americans and lawful residents who carry state-issued driver's licenses or ID cards. Neither the Act nor the accompanying regulations placed any limits on the permissible uses of the REAL ID card, giving unfettered discretion to DHS to expand the "official purposes" for which REAL ID cards could be required, thus creating a serious risk of "mission creep." If merchants and other third parties are free to ask for the card and collect data from it, there is a very real possibility that individuals would not be able to function in American society without a REAL ID card.

- **Create a centralized ID database**: The Bush Administration adamantly denied it, but REAL ID would likely result in the creation of a central ID database (or system of databases) by, among other things, requiring that states "provide electronic access" to all other states to information contained in motor vehicle databases. Intended to support the goal of "one driver, one license," such a centralized repository of identity information would be both unnecessary and especially vulnerable to hackers, identity thieves, and internal abuse.

- **Incorporate no meaningful privacy protections**: REAL ID adopted no meaningful privacy and security standards for the protection of personal information stored in the REAL ID system. The Act itself doesn't require any privacy or security safeguards for information collected and stored pursuant to the program. While DHS's regulations required that states develop a privacy policy and adopt reasonable safeguards to protect PII, the regulations did not provide any specific benchmarks against which DHS could assess states' compliance.

---

7 Center for Democracy & Technology, "Three Years Later: A Primer on REAL ID" (August 2008), http://www.cdt.org/publications/policyposts/2008/13.

- **Mandate a standardized, unprotected MRZ**: Finally, REAL ID mandated a standardized MRZ, with no requirement of encryption and no limits on the data elements it could contain. In addition, there are no limits on who can scan the MRZ, collect personal information, and record the cardholder's activities. The lack of security and privacy safeguards for the MRZ would facilitate intrusive tracking and profiling by both private third parties and unauthorized government entities.

At heart, not only would various mandates in the program be ineffective at making ID card and license issuance more secure, REAL ID created new privacy and security risks while exacerbating existing ones. CDT concluded that the REAL ID Act was so fundamentally flawed that changing DHS's regulations alone would be insufficient to address the serious risks posed.[8]

Recognizing the unfunded (and high) costs of the program and its impact on privacy and civil liberties, the states responded negatively to REAL ID, ranging from outright rejection of implementation to legislative resolutions expressing disapproval. The Bush Administration delayed implementation of the program, essentially passing to this Congress and the new Administration the question of how to proceed.

Enhanced Driver's Licenses and Passport Cards

REAL ID is not the only problematic ID card program. In a related initiative, several states are currently issuing enhanced driver's licenses (EDLs) with imbedded, insecure RFID chips as part of the Western Hemisphere Travel Initiative (WHTI). The long range (so-called "vicinity-read") RFID chip that DHS chose for this initiative is highly insecure. The technology was designed for tracking inventory, not people, and can consequently be read from a considerable distance by third parties using standardized and widely available equipment. The State Department's passport card also incorporates these insecure RFID chips.

When used for human identification, long range or vicinity-read RFID poses serious threats to personal privacy and security: it reduces user notice and control over when information is collected from the card and enables location tracking of the cardholder because the unique identifier stored on the chip can be easily skimmed (if unencrypted). These serious risks make such long range

8 Center for Democracy & Technology, "REAL ID: What Should Congress Do Now? CDT Analysis of the REAL ID Act and the Department of Homeland Security's Final Regulations" (Feb 2008), http://www.cdt.org/security/identity/20080201_REAL_ID_hillbrief.pdf.

RFID technology inappropriate for human identification and far outweigh the justifications asserted for its use in the EDL and passport card initiatives.[9]

The PASS ID Act [S. 1261] Mitigates Major Privacy Issues REAL ID Raises

The Providing for Additional Security in States' Identification (PASS ID) Act [S. 1261] mitigates key privacy and security flaws in the REAL ID program. The approach the Act proposes will increase the reliability of driver's licenses and ID cards in a way that better protects privacy and civil liberties. CDT supports the adoption of the PASS ID Act as a much-needed improvement over current law.

Most notably, the PASS ID Act:

- **Removes the requirement that states "provide electronic access" to all other states to information contained in motor vehicle databases.** Instead, to ensure "one driver, one license," the Act takes a much less onerous and less privacy invasive approach, requiring states to "[e]stablish an effective procedure to confirm" that a person applying for a compliant license or ID card is terminating or has terminated any other compliant license or card issued by another state. This change takes away one impetus for further centralization of identity data. [Sec. 3 - §242(d)(5)]

- **Removes from DHS's independent authority the ability to determine new "official purposes" for which a compliant ID can be required.** PASS ID would require compliant cards for three specified official purposes and removes from DHS's authority the ability to unilaterally determine additional purposes (as REAL ID allowed). This change mitigates (though does not eliminate) the risk of mission creep. [Sec. 3 - §241(4)]

- **Requires privacy and security protections for PII in back-end systems.** The PASS ID Act requires states to establish administrative and physical safeguards to protect the PII collected and maintained for license and ID card issuance. The Act also specifies that states must have procedures to prevent unauthorized access to and use of PII; give public notice of

9 Center for Democracy & Technology, CDT Testimony on "The Impact of Implementation: A Review of the REAL ID Act and the Western Hemisphere Travel Initiative" (April 2008), available at http://www.cdt.org/testimony/20080429scope-written.pdf.

security and privacy policies; and establish a process for cardholders to access and correct their own PII. [Sec. 3 - §242(d)(7)]

- **Provides protections for personal information on the MRZ.** While the PASS ID Act still mandates the use of an MRZ, it prohibits the inclusion of the cardholder's Social Security number in the zone [Sec. 3 - §242(b)(9)] and places limits on the storage, use, and redisclosure of information contained in the MRZ. [Sec. 4]

In addition, the PASS ID Act would establish a State-to-State One Driver, One License demonstration project to evaluate the feasibility of establishing an electronic system to prevent an individual from obtaining more than one PASS ID-compliant driver's license or ID card at any one time. [Sec. 3 - §245] The project would include a review of the appropriate governance structures that will be necessary to prevent unauthorized use of PII in the system and to ensure its security and confidentiality.

Privacy Protections Could be Further Strengthened in PASS ID

While the PASS Act does not address all flaws in the REAL ID program, merely repealing REAL ID does not address all of the underlying privacy and security risks posed by government identification programs. PASS ID provides the opportunity to start building privacy guidance and protections into all state identification programs, addressing trends and issues that will exist regardless of REAL ID implementation.

There are a number of ways in which the PASS ID bill could be further strengthened to protect privacy and civil liberties, while still achieving security objectives. Specifically, CDT urges Congress to:

- Repeal the mandate for a standardized MRZ. Congress probably should not prohibit the trend towards inclusion of MRZs on state driver's licenses, but it should not be promoting this trend either. States should have the ability to consider and reject the use of MRZs if they determine the risks to privacy and security outweigh the benefits to their citizens.

- To the extent that states wish to include an MRZ, mandate encryption or other security features for the MRZ so that data cannot be read or used for unauthorized purposes.

- Limit the data elements that may be contained on the MRZ to only what is necessary for legitimate law enforcement or DMV administrative purposes.[10] The less information contained in the MRZ, the less attractive skimming will be to unauthorized third parties.

- Reject the use of "vicinity-read" RFID technologies (now incorporated in EDLs and passport cards) in PASS ID-compliant driver's licenses and ID cards.[11]

- Require encryption to protect any PII transmitted electronically for PASS ID compliance.[12]

- Remove or substantially shorten the retention requirement for physical or electronic copies of source documents.[13] Central retention of such sensitive documents creates a treasure trove of information that would attract identity thieves and facilitate internal fraud.

Finally, Congress should strengthen privacy protections for all Americans and lawful residents who carry government-issued identity credentials, regardless of PASS ID implementation, by shoring up the Driver's Privacy Protection Act (DPPA). The DPPA is the main federal law protecting personal data in state DMV databases from disclosure to third parties. However, the DPPA contains a myriad of exceptions that virtually swallow the rule against disclosure of such data. Congress should amend the DPPA to protect against both governmental and commercial abuse of information by closing the loopholes it currently contains.

Congress should also directly address the privacy risks associated with state trends towards outsourcing management of personal information to private entities such as the American Association of Motor Vehicle Administrators (AAMVA). Congress should amend the DPPA to clearly extend application of protections to information systems managed by private, non-governmental entities to ensure uniform protection for all driver's license information.

---

10 This could be accomplished by amending § 242(b)(9) in the proposed Title II, Subtitle E of the Homeland Security Act.

11 This could be accomplished by amending § 242(a)(4) in the proposed Title II, Subtitle E of the Homeland Security Act.

12 This could be achieved in Sec. 5(b)(2) of the PASS ID Act.

13 This could be addressed in § 242(d)(1) in the proposed Title II, Subtitle E of the Homeland Security Act.

Conclusion

Protecting privacy and security in identification programs is an ongoing process that requires continual attention to new risks, including the potential for third party profiling and fraud. The PASS ID Act would be a notable improvement over current law and provides an opportunity to start building in privacy guidance to address privacy and security risks that exist apart from REAL ID. The new bill incorporates nearly all of the substantial privacy protections from the REAL ID repeal bill that CDT supported in front of this committee in the 110th Congress and a few more. Most importantly, PASS ID: 1) removes the requirement that states provide electronic database access to other states; 2) takes away DHS's unilateral, independent authority to determine new purposes for a compliant ID; 3) requires privacy and security safeguards for information in back-end databases; and 4) imposes prohibitions on skimming and use of MRZ data.

CDT urges the Committee to ensure that these provisions are not weakened. We stand ready to work with Members of the Committee to improve privacy and security in driver's license and ID card issuance and in associated back-end information systems. Thank you again for the opportunity to testify.