

---

# PASS ID Act Addresses Major Privacy Concerns in REAL ID

June 14, 2009

*Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts [here](#):*

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 plug the security gaps identified by the 9/11 Commission. Alongside these initiatives, states have been redesigning their driver's license systems to incorporate advanced technology features.

[1\) Government ID Card Programs Raise Privacy Concerns](#)

[2\) REAL ID and Enhanced Driver's Licenses Exemplify Concerns](#)

[3\) Proposed PASS ID Act Offers Much-Needed Improvements](#)

[4\) Protecting Privacy Will Require Additional Reforms](#)

---

## 1) Government ID Card 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 plug the security gaps identified by the 9/11 Commission. Alongside these initiatives, states have been redesigning their driver's license systems to incorporate 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, security, and other civil liberties 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 ways that are unprotected and interoperable;
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 to facilitate 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).

---

## 2) REAL ID and Enhanced Driver's Licenses Exemplify Concerns

REAL ID (as defined by the REAL ID Act and DHS's final regulations) and the related Enhanced Driver's License (EDL) initiative exemplify the problematic trends in government identity programs.

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 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.

More importantly, the REAL ID approach presented critical privacy and security risks:

- The REAL ID Act created a de facto national ID card for the 240 million Americans and lawful residents who carry state-issued driver's licenses or ID cards. Moreover, 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."
- REAL ID would likely result in the creation of a central ID database (or system of databases) by requiring that states "provide electronic access" to all other states to information contained in the motor vehicle databases. Intended to support the goal of "one driver, one license," such a centralized repository of identity information is both unnecessary and would be vulnerable to hackers, identity thieves, and internal abuse.
- 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 require that states develop a privacy policy and adopt reasonable safeguards to protect PII, the regulations do not provide any specific benchmarks against which DHS can assess states' compliance.
- Finally, REAL ID mandated a standardized MRZ, with no requirement of encryption and no limitations on the data elements it can contain. In addition, there are no limitations 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 will 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 would also create new privacy and security risks while exacerbating existing ones. Recognizing the unfunded (and high) costs of the program and its impact on privacy and civil liberties, the states have responded negatively to REAL ID, ranging from outright rejection of implementation to non-binding legislative resolutions formally expressing disapproval. CDT has concluded that the REAL ID Act is so fundamentally flawed that changing DHS's regulations alone would be insufficient to address the serious privacy and security concerns posed.

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 ("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. When used for human identification, it 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 RFID technology inappropriate for human identification and far outweigh the justifications asserted for its use in the EDL.

[CDT Analysis](#) [1] of DHS Final Regulations and Recommendations for Congress (Feb. 2008)

[Three Years Later: A Primer on REAL ID](#) [2] (Aug. 2008)

[CDT Testimony](#) [3] on "The Impact of Implementation: A Review of the REAL ID Act and the Western Hemisphere Travel Initiative"

---

### **3) Proposed PASS ID Act Offers Much-Needed Improvements**

On June 15, 2009, Senators Akaka (D-HI), Baucus (D-MT), Carper (D-DE), Tester (D-MT), and Voinovich (R-OH) introduced the Providing for Additional Security in States' Identification (PASS ID) Act of 2009. The bill addresses most of the major concerns CDT has raised regarding REAL ID. The approach the Act proposes will go a long way towards increasing the reliability of driver's licenses

and ID cards in a privacy and civil liberties protective way.

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 “establish 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. [Sec. 3 - §242(d)(5)]
- **Limits the “official purposes” for which a compliant ID can be required by a federal agency.** PASS ID would require compliant cards for three specified official purposes and denies DHS the authority to unilaterally determine additional purposes. [Sec. 3 - §241(4)] In addition, PASS ID provides that no person can be denied boarding a commercial aircraft solely on the basis that they fail to present a PASS ID-compliant credential. [Sec. 3 - §242(a)(1)(B)]
- **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 at locations where licenses and ID documents are produced or stored. The Act also specifies that states must have procedures to prevent unauthorized access to and use of PII; give public notice of 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 MRZ [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 driver's license or ID card at any one time [Sec. 3 - §245]. The project will 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.

---

## 4) Protecting Privacy Will Require Additional Reforms

CDT has long promoted the goal of making driver's license and ID card issuance more secure, as recommended by the 9/11 Commission. CDT supports the adoption of the PASS ID Act because it corrects key privacy security flaws in the REAL ID program and is a much-needed improvement over current law.

However, work still needs to be done to ensure robust privacy protections for the 240 million Americans and lawful residents who carry government-issued identity credentials. Protecting privacy and security is an ongoing process that requires continual attention to new risks and the potential for third party profiling and fraud. CDT will continue to work with Congress and the states to improve privacy and security in driver's license and ID card issuance and in associated back-end information systems.

Specifically, as PASS ID moves forward, CDT urges Congress and DHS to continue to keep in mind the lessons learned from previous ID card programs (especially REAL ID):

- Write regulations that would have the backing of all relevant stakeholders, including the various states and individual rights advocates.
- In the regulations and as part of the One Driver, One License demonstration project, specify clearly the permissible purposes and users of PII in the MRZ and in back-end databases and adopt procedures to prevent unauthorized uses.
- Reject the use of “vicinity-read” RFID technologies (now incorporated in EDLs and



passport cards) in future ID programs and allow states to give their citizens the choice of applying for a PASS ID-compliant card that does not incorporate "vicinity-read" RFID.

---

Copyright © 2008 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

**Source URL:** <https://www.cdt.org/policy/pass-id-act-addresses-major-privacy-concerns-real-id>

**Links:**

- [1] [http://www.cdt.org/security/identity/20080201\\_REAL\\_ID\\_hillbrief.pdf](http://www.cdt.org/security/identity/20080201_REAL_ID_hillbrief.pdf)
- [2] <http://www.cdt.org/publications/policyposts/2008/13>
- [3] <http://www.cdt.org/testimony/20080429scope-written.pdf>