More on PASS ID: Strengthening Privacy Protections for REAL Progress

July 8, 2009

Three weeks ago, the PASS ID Act [S. 1261] [1] was introduced in an effort to move beyond the REAL ID stalemate [2] that has dragged on for over three years. CDT supports PASS ID [3] because it mitigates key privacy flaws in the REAL ID program and is a notable improvement over current law. While the privacy provisions in PASS ID can still be strengthened, the bill incorporates nearly all the privacy requirements that the last Congress's REAL ID repeal act [4] included [S. 717, 110th] and was even introduced by the same Senator, Daniel Akaka (D-HI).

Putting aside for a moment the question of whether repeal of REAL ID is a political possibility, it is important to realize that repeal is not necessarily better than REAL ID: 1) Senator Akaka's repeal act would not have stopped the creation of new licensing standards, it would simply have created a negotiated rulemaking body that would have had to use exactly the same standards that are in his PASS ID Act to help increase privacy; 2) If we could re-write the repeal bill to not incorporate any new standards, it would still not address the problem that state driver's license programs have already been moving towards greater standardization of design and interoperability of technological features for quite some time with limited privacy and security protections. CDT remains concerned about three main trends happening at the state level:

- States are incorporating machine-readable zones (MRZ) [5] in driver's licenses and ID cards, without encryption or other protections for the information contained in the zone.
- Because personally identifiable information (PII) contained in the MRZ is unprotected and the technologies interoperable, information in the MRZ can be read, stored, and re-used with few limitations by commercial and governmental entities.
- ID card systems have increasingly centralized back-end information systems containing vast amounts of identity data, vulnerable to theft or internal abuse if not properly protected. States are also turning to private, non-governmental agencies such as AAMVA [6] to manage such systems.

In addition, the use of facial imaging is already widespread among states. REAL ID in many ways exemplifies these trends, but the privacy and civil liberties risks these trends implicate would still exist whether REAL ID is repealed or stays on the books. CDT believes these concerns should be addressed for all states, regardless of REAL ID implementation and regardless of whether REAL ID is repealed. PASS ID would help accomplish this important goal. These questions become even more salient when back-end information systems are managed by private, non-governmental agencies (for example, AAMVA) because no robust legal framework for privacy protection applies directly to such entities: The Privacy Act may not apply to a database managed by a state or private entity. And while the Driver's Privacy Protection Act (DPPA) [7] applies to state DMVs and their contractors, the protections that the DPPA offers are woefully incomplete at best. PASS ID does not fix everything that worries privacy advocates about REAL ID. However, privacy advocates still have the opportunity to encourage changes and to build in stronger privacy guidance and protections to address state trends that exist regardless of REAL ID. In particular, CDT urges Congress to strengthen privacy in PASS ID by:

- Mandating encryption or other security features to protect against unauthorized scanning of information in the 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. [§ 242(b)(9)] The less information contained in the MRZ, the less attractive skimming will be to unauthorized third parties.
- Rejecting the use of "vicinity-read" RIFD technologies (now incorporated in EDLs) in PASS ID

cards. [§ 242(a)(4)]
- Requiring encryption to protect any PII transmitted electronically for PASS ID compliance purposes. [Sec. 5(b)(2)]
- Removing or substantially shortening the retention requirement for physical or electronic copies of source documents. [§ 242(d)(1)] Central retention of such sensitive documents creates a treasure trove of information that would attract identity thieves or facilitate internal fraud.

We will continue to push for the inclusion of these changes.

In the end, however, privacy advocates will have to decide whether the word "repeal" or the protections that could realistically come from a repeal are more important. CDT would prefer to see progress than to fight for a meaningless distinction.

- REAL ID ACT
- tbp
-
- privacy
- PASS ID Act
- Congress
- Driver's license
- CDT

Source URL:
https://cdt.org/blogs/cynthia-wong/more-pass-id-strengthening-privacy-protections-real-progress

Links:
[1] http://thomas.loc.gov/cgi-bin/query/z?c111:S.1261:
[2] http://www.cdt.org/publications/policyposts/2008/13
[3] http://blog.cdt.org/2009/06/15/pass-id-act-offers-real-reforms/
[4] http://thomas.loc.gov/cgi-bin/query/z?c110:S.717:
[5] http://www.aamva.org/KnowledgeCenter/Standards/uslicensetechnology.htm
[6] http://www.aamva.org/TechServices/
[7] http://www.cdt.org/privacy/guide/protect/laws.php#dpp