

1634 I Street, NW Suite 1100 Washington, DC 20006 202.637.9800 fax 202.637.0968

## PASS ID Act of 2009 Overview June 2009

On June 15, 2009, Senators Akaka, Voinovich, Leahy, Tester, Baucus and Carper introduced the Providing for Additional Security in States' Identification (PASS ID) Act of 2009. 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 mitigates or corrects key privacy and security flaws in REAL ID:

REAL ID Act of 2005	PASS ID Act of 2009
Mandated that each state give every other state "electronic access" to their motor vehicle database (i.e., people's records) with the ostensible but unstated limited purpose of ensuring that no driver holds more than one license. [§202(d)(12)]  Considering the Act provided no limits on what information can be shared and with whom, this provision would likely result in the creation of a central ID database. Such a centralized repository of identity information is unnecessary and would be vulnerable to hackers, identity thieves, and internal abuse.	Removes the requirement that states "provide electronic access" to all other states to information contained in state 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.  [Sec. 3 - §242(d)(5)]
Provided no statutory limitations on the "official purpose" for which a federal agency can require a REAL ID and gave the Secretary of Homeland Security unfettered discretion to determine new purposes. [§202(a)(1)]  Without limitations on required uses, the REAL ID card would become the <i>de facto</i> national ID card and creates a serious risk for "mission creep."	Limits the "official purposes" for which a compliant ID can be required by a federal agency. [Sec. 3 - §241(4)]  PASS ID lists three specified official purposes – accessing federal facilities critical to homeland security, accessing nuclear power plants, and boarding federally regulated commercial aircraft – and denies DHS the authority to unilaterally determine additional purposes.  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)]

Mandated that each state give every other state "electronic access" to the database (i.e., people's records) and without statutory limitations on what information can be shared between states and for what purposes; who else (e.g., other state agencies, federal agencies, third parties) can access the databases and for what purposes. [§202(d)(12)]

The REAL ID Act and its implementing regulations provided no meaningful privacy and security standards for the protection of PII contained in the REAL ID system. While DHS's regulations required states to develop a privacy policy and adopt reasonable safeguards, the regulations provided no benchmarks against which DHS can assess state compliance.

Mandated that each card have Machine Readable Technology (MRT) and did not provide any statutory limitations on *what* information is stored in the Machine Readable Zone (MRZ), *who* can "skim" information from the MRZ (e.g., state agencies, federal agencies, third-parties) and for *what purposes*. REAL ID also provided no statutory security requirements such as encryption. [§202(b)(9)]

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.

Statutorily requires safeguards for the PII collected and maintained in back end databases for the program. [Sec. 3 - §242(d)(7)]

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.

Mandates the use of a common MRT and does not impose security requirements, but **provides** additional protections for PII contained in the MRZ. [Sec. 3 - §242(b)(9); Sec. 4]

The PASS ID Act forbids states from including the cardholder's social security number in the MRZ on a license or ID card. [Sec. 3 - §242(b)(9)]

In addition, PASS ID amends the Driver's Privacy Protection Act, 18 U.S.C. § 2721 et. seq. (Pub. L. 103-322), to impose penalties for the storage, use, and disclosure of information contained on the MRZ by any person without lawful authority to do so. [Sec. 4]