Three Years Later: A Primer on REAL ID

August 28, 2008

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

The 9/11 Commission Report highlighted the need for increased security when issuing driver's licenses and ID cards in the United States. In response, Congress passed the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. Among other provisions, the law called for a negotiated rulemaking to create new federal standards for state driver's licenses nationwide. Notably, the rulemaking process included state DMV representatives, state elected officials, the Department of Homeland Security (DHS), and other interested parties (among them, CDT and ACLU representatives) in the negotiations. Such a rulemaking process allowed for cooperation among various stakeholders and appropriately recognized that driver's licenses have historically been an area of state concern.

---

(1) The REAL ID Act Repealed the Promising Negotiated Rulemaking Process

The 9/11 Commission Report highlighted the need for increased security when issuing driver's licenses and ID cards in the United States. In response, Congress passed the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. Among other provisions, the law called for a negotiated rulemaking to create new federal standards for state driver's licenses nationwide. Notably, the rulemaking process included state DMV representatives, state elected officials, the Department of Homeland Security (DHS), and other interested parties (among them, CDT and ACLU representatives) in the negotiations. Such a rulemaking process allowed for cooperation among various stakeholders and appropriately recognized that driver's licenses have historically been an area of state concern.

However, before the negotiated rulemaking process could be completed, Congress halted the process with the passage of the REAL ID Act of 2005, adding the Act as a rider to a war and tsunami relief appropriations bill. The Senate never held any hearings or debated REAL ID, and the entire measure was passed quickly due to the urgency surrounding the main bill. Thus, REAL ID came into force not through independent or well-reasoned assessment, but rather through political gamesmanship.

In addition to repealing the negotiated rulemaking process in IRTPA, Title II of the REAL ID Act created new federal standards for state-issued driver's licenses and ID cards, and enabled DHS to issue regulations to implement the law, without also mandating that the privacy of cardholders be respected.

States have reacted negatively to REAL ID for various reasons, including: concerns about privacy, that REAL ID would create a national ID card, and that the federal government has imposed an unfunded mandate. So far, 11 states have passed laws barring REAL ID compliance, and an additional 10 states have formally expressed displeasure with REAL ID (for example, with non-binding resolutions).

The deadline for compliance with REAL ID was originally slated for May 8 of this year, but DHS did not issue its proposed regulations until March 2007. After receiving more than 21,000 responses

during the comment period, the Department did not publish its final regulations until January 2008. In April of 2008, DHS announced that all 56 U.S. jurisdictions subject to REAL ID had been granted an extension until December 31, 2009, with the possibility of applying for a second extension until May 10, 2011 if they show "material compliance" with the Act. Oddly, even states that did not seek an extension or had actively opposed REAL ID's implementation were granted extensions.

CDT Statement for the Record on REAL ID [1] (March 2007)

DHS REAL ID Final Regulations [2] (Jan. 2008)

---

(2) REAL ID Poses Serious Privacy and Security Risks

A significant privacy and civil liberties risk stemming from the REAL ID Act is that it will create a de facto national ID card for the more than 240 million Americans who carry state-issued driver's licenses or ID cards. Neither the Act nor the accompanying DHS regulations place any limits on the permissible uses of the REAL ID card by governmental or commercial entities; DHS explicitly stated in its final regulations that it has neither the power nor interest in limiting such uses. Furthermore, DHS has retained unfettered discretion to expand the definition of "official purpose" for which REAL ID cards will be required. The final regulations require REAL IDs for access to federal facilities, boarding commercial aircraft, and entering nuclear power plants; however, the regulations give DHS the option of expanding the mandatory use of REAL ID's for other, as yet undefined, purposes.

Thus, there is a high risk of "mission creep" with respect to REAL ID. Just five days after the final regulations were published, a senior DHS official publicly suggested that REAL ID could help fight the methamphetamine crisis. This follows earlier congressional proposals to require a REAL ID card for a myriad of different purposes, including employment, federal housing benefits, and voting. DHS' Data Privacy & Integrity Advisory Committee (DPIAC) also expressed concerns over the potential for mission creep, recommending that DHS place "restrictions on unilateral authority to change required uses for the REAL ID cards." DHS ignored that advise when writing the final regulations for the use of REAL IDs.

It is ironic that REAL ID moves the nation closer toward a national ID card while Congress and federal agencies have been striving to reduce the use of the Social Security Number, which has been the de facto national identifier and a key facilitator of identity theft over the past several decades.

The proposed implementation of REAL ID will also result in the creation of a central ID database (or system of databases), which will threaten the privacy and security of over 240 million Americans. By developing a single database for all drivers and ID card holders, or by requiring that all state motor vehicle databases be linked, REAL ID will create a massive and potentially vulnerable centralized repository of highly sensitive personal information on almost every American. It is likely that DHS will contract the running of such a database to a private entity; however, there is no robust legal framework that would ensure the security and protect the privacy of personal information stored in such a centralized ID system. Federal laws like the Privacy Act and the Driver's Privacy Protection Act likely would not apply to a database managed by a private entity such as the American Association of Motor Vehicle Administrators (AAMVA) and so would not provide adequate privacy protections for personal information in such a database. Such a centralized ID system would be a "one stop shop" and treasure trove of valuable information for identity thieves, terrorists, and unscrupulous government employees.

DHS' final regulations also fail to limit government access to information held in any kind of central ID system created under REAL ID, nor do they limit what information will go into the central database nor prohibit the collection or storage of additional information about individuals. This could lead to an

expansion over time of the central ID database to include increasingly detailed information on American citizens including their movements and activities, which would be a clear violation of personal privacy.

Another privacy and security risk stems from DHS' mandate that every card have a standardized, unencrypted Machine-Readable Zone (MRZ). DHS's DPIAC called for adding security safeguards to "prevent unauthorized access to information on the card, including any contained in the . . . MRZ," but DHS failed to heed this advice in adopting its final regulations. The MRZ will facilitate intrusive tracking by both government and commercial entities. Innumerable state and federal agencies, as well as businesses and non-governmental third parties, could scan the MRZ, collect personal information, and record individuals' activities. The private sector could also scan the MRZ during the course of ordinary commercial activities and develop profiles of consumer behavior. The DHS final regulations do nothing to prohibit any of this type of activity. Furthermore, neither the Act nor the final regulations restrict what personal information may be stored in the MRZ, leaving open the potential for detailed records about an individual to be stored in an unencrypted format accessible to anyone who has a standard reader. DHS' DPIAC also called for "restrictions on unauthorized uses, including commercial uses as a standard identifier" and for minimizing the data stored in the MRZ.

Finally, DHS failed to adopt meaningful privacy and security standards for the protection of personal information stored in the REAL ID system. The REAL ID Act itself does not require that personal information, which includes copies of source documents such as birth certificates and passports collected and stored pursuant to the Act, be protected by privacy and security safeguards. To its credit, DHS has interpreted its authority to include the power to require states to develop a privacy policy and institute "reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable information." However, the final regulations fail to include specific privacy and security safeguards against which DHS will gauge states' compliance with the REAL ID Act. DHS' DPIAC also noted this shortcoming in its comments on the proposed regulations.

DHS Data Privacy & Integrity Advisory Committee Comments on Proposed REAL ID Regulations [3] (May 2007)

---

(3) Congress Must Act to Address the Problems With REAL ID

The REAL ID Act is so fundamentally flawed that altering DHS' regulations alone would be insufficient. Congress must act to address the serious risks posed by REAL ID.

CDT supports three options for REAL ID legislative reform. CDT has consistently supported the Identification Security Enhancement Act of 2007, introduced by Sen. Daniel Akaka (D-HI), which would repeal Title II of the REAL ID Act and replace it with a negotiated rulemaking committee. In addition, the Akaka bill would add language emphasizing the need to include "experts in privacy protection, experts in civil liberties and protection of constitutional rights, and experts in immigration law" in the rulemaking process. The bill also explicitly provides for federal grants to underwrite the costs of complying with new minimum federal standards for driver's licenses. Passage of this bill would represent a return to the process originally called for in the Intelligence Reform and Terrorism Prevention Act 2004. A negotiated rulemaking committee could:

- Develop meaningful federal minimum standards that would actually make driver's license issuance more secure and the card a more reliable assertion of identity;
- Write regulations that would have the backing of all relevant stakeholders, including the various states (both those in favor of REALD ID, and, hopefully, the 21 states that have

actively opposed REAL ID) and individual rights advocates; and
- Still promote implementation of reforms on a schedule faster than what DHS proposes for REAL ID.

Alternatively, Congress could amend REAL ID to address specific privacy and security risks. The following reforms would work to ensure security and protect the privacy of American citizens:

- Prohibit expanded required uses of the REAL ID card and include statutory language that specifically prohibits card numbers from being unique across the nation;
- Prohibit the creation of a central ID database;
- Repeal the mandate for a standardized MRZ;
- Limit the personal information that can be stored in the MRZ;
- Mandate encryption and other security features for the MRZ and computer systems;
- Prohibit state and federal agencies, as well as business and other private organizations, from scanning the REAL ID card to collect personal information or track individuals' activities; and
- Amend the Driver's Privacy Protection Act to clearly address the issue of personal ID information managed by a private entity such as AAMVA.

A third option for Congress would be to repeal the REAL ID Act and replace it with a simplified law that focuses on source document verification, which is perhaps the most useful reform to ensure that people are who they say they are. Congress could change how it exercises authority over the states, shifting from invoking the right to regulate IDs used for federal purposes to conditioning the receipt of federal monies on states taking certain driver's license reform actions. Additionally, Congress could mandate specific privacy and security standards for the protection of personal information, which could come in the form of amendments to the Driver's Privacy Protection Act.

CDT Analysis of DHS Final Regulations and Recommendations for Congress [4] (Feb. 2008)

Source URL: https://www.cdt.org/policy/three-years-later-primer-real-id

Links:
[1] http://www.cdt.org/security/identity/20070326cope.pdf
[2] http://a257.g.akamaitech.net/7/257/2422/29jan20081800/edocket.access.gpo.gov/2008/08-140.htm"
[3] http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_05-2007_realid.pdf
[4] http://www.cdt.org/security/identity/20080201_REAL