

April 8, 2008

Chairman Patrick Leahy  
Ranking Member Arlen Specter  
Senate Judiciary Committee  
224 Dirksen Senate Office Building  
Washington, DC 20510

Dear Chairman Leahy and Ranking Member Specter:

We write to respond to Department of Homeland Security (“DHS”) Secretary Michael Chertoff’s factual assertion during a Judiciary Committee hearing on DHS oversight on April 2 that it will be impossible for third parties to “skim” personal information from REAL ID cards, and thus the risks to personal privacy of requiring a standardized “machine-readable zone” are nonexistent. This statement is factually incorrect.

It may be that the Secretary was misinformed about the technology at issue. But to get the facts completely wrong, while at the same time accusing privacy advocates of being “dead wrong” and putting out “misinformation” about the privacy and civil liberties risks of REAL ID, strains credulity. This Committee and the public deserve better.

Specifically, Secretary Chertoff stated that there will be no risk of the wrong people gaining access to personal information stored in the REAL ID card’s “machine-readable zone” (MRZ) because the skimming of personal information is only a risk associated with RFID chips. He testified, “You cannot skim a machine-readable zone because skimming, to the extent it occurs, requires an RFID chip, and a machine-readable zone is not an RFID chip. And we are not requiring RFID chips.”

In fact, an RFID chip is a kind of “machine-readable zone,” but it is not the only kind of MRZ from which personal information can be skimmed.<sup>1</sup> An MRZ is a section of an ID card that

---

<sup>1</sup> CDT supports DHS’ decision *not* to mandate an RFID chip in REAL ID cards, which would present an even greater privacy risk since RFID chips can be read remotely and without the knowledge of the cardholder.

stores digitized personal data that can be quickly scanned and collected by a widely available electronic reader. Other MRZ examples are the common magnetic stripe like those on credit cards or the one-dimensional (1D) bar code like those on grocery packages. Police officers regularly scan the various MRZs of existing state driver's licenses, as do businesses such as bars that seek to verify that patrons are over 21.

The REAL ID Act mandates that state driver's licenses and ID cards include a standardized machine-readable zone. DHS' implementing regulations mandate the 2D barcode as the MRZ technology but fail to require that the personal information stored in the MRZ be encrypted or otherwise protected from unauthorized use – despite extensive comments from privacy advocates to do just that.<sup>2</sup> 2D barcode readers are already widely available, and mandating that all REAL ID driver's licenses and ID cards use the *same unsecured* MRZ technology will make the use of the readers even more ubiquitous, thus increasing the risk to personal privacy.<sup>3</sup>

The legislative history of the REAL ID Act makes clear that the MRZ was intended only to be a law enforcement tool,<sup>4</sup> yet DHS' regulations make no effort to protect the personal information that will be digitally stored on the REAL ID cards from collection by non-law enforcement parties. The fear that businesses and government agencies alike will increasingly scan the 2D barcode, collect and possibly resell personal information, and log the activities and movements of innocent Americans is not unwarranted. Yet Secretary Chertoff responded to Senator Feingold that it is a “blatant falsehood” that REAL ID cards could be used to track people.

CDT outlined the risks of a standardized, unencrypted machine-readable zone in the comments submitted to DHS on the proposed REAL ID regulations last year,<sup>5</sup> as well as in a recent analysis of the final REAL ID regulations. That analysis also includes recommendations for much-needed Congressional action to fill the privacy and security gaps created by REAL ID.<sup>6</sup>

The issues presented by the mandated use of a standardized, unsecured MRZ technology – whether the 2D barcode or otherwise – is real, but DHS has failed to address the issue of MRZ security, leaving the problem to the states. If the federal government is going to get into the

---

<sup>2</sup> DHS' final REAL ID regulations at 5292, <http://a257.g.akamaitech.net/7/257/2422/29jan20081800/edocket.access.gpo.gov/2008/08-140.htm>.

<sup>3</sup> A related privacy risk involves the amount and type of personal data required to be digitally stored in the 2D barcode. The REAL ID Act requires that the MRZ contain “minimum data elements” and DHS has defined these as: expiration date, full legal name, date of transaction, date of birth, gender, address, unique driver's license or ID card number, card revision date, inventory control number of the physical document, and state of issuance. CDT has consistently argued that storing only the minimum amount of personal information needed by law enforcement in the MRZ, such as name and driver's license number, will help protect personal privacy; as would granting states discretion in what personal data will be stored in the MRZ, even if it is none at all.

<sup>4</sup> Conference Report on H.R. 1268, House Report 109-72 at 179.

<sup>5</sup> <http://www.cdt.org/security/20070508realid-comments.pdf>.

<sup>6</sup> [http://www.cdt.org/security/identity/20080201\\_REAL\\_ID\\_hillbrief.pdf](http://www.cdt.org/security/identity/20080201_REAL_ID_hillbrief.pdf).

business of regulating state driver's licenses, then it has an obligation to make sure personal privacy is protected.

We strongly urge the Committee to ask Secretary Chertoff to correct the record with respect to his testimony of April 2 on the privacy implications posed by the use of the unencrypted 2D barcode. We further ask this Committee to quickly address the privacy and security gaps in the REAL ID Act and implementing regulations.

Sincerely,

Sophia Cope  
Staff Attorney/Ron Plesser Fellow  
Center for Democracy & Technology

cc: Members of the Senate Judiciary Committee