



April 7, 2006

Secretary Michael Chertoff
U.S. Department of Homeland Security
Department of Homeland Security
Nebraska Avenue Center, NW
Washington, D.C. 20528

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
TECHNOLOGY AND
LIBERTY PROGRAM
NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2559
F/212.549.2629
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
NADINE STROSSEN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

KENNETH B. CLARK
CHAIR, NATIONAL
ADVISORY COUNCIL

RICHARD ZACKS
TREASURER

Re: Real ID Act of 2005, Regulations

Dear Secretary Chertoff:

We expect that the Department of Homeland Security will soon issue regulations implementing the Real ID Act of 2005. We are writing to urge the Agency to adopt reasonable privacy standards to protect US drivers and identification holders from intrusions by the government, private industry and identity thieves.

As the ACLU has made clear in several meetings with the Department, we believe the Real ID Act represents one of the most significant threats to the privacy of Americans in recent memory. With this legislation, Congress has created a massive new system of over 200 million standardized driver's licenses backed up by a database that will include virtually every competent American. Yet Congress created only the most general of guidelines for this enormous new system, granting DHS broad authority to actually implement it.

What Real ID Does

Following are the main elements of the Real ID Act that have to do with National ID cards. Real ID:

- **Standardizes data.** Requires that driver's licenses include a wide and standard set of personal data including name and address, date of birth, a biometric identifier, unique ID number and physical description.
- **Mandates a "machine-readable technology."** Requires that the data be made available not only on the front of the card, but also on an undefined machine-readable technology included in the card. That is significant because it could make it easy for private industry to snap up the data on these IDs, intensifying

the collection and trading in private data and to the creation of a parallel database not subject even to the limited privacy rules in effect for the government.

- **Creates a single national database.** Real ID forces states to link their driver databases (databases that contain detailed personal data on every licensed driver) with other states and the Federal Government. This creates, in effect, a single seamless national database, so that all of the private data in motor vehicle records is instantly available to a wide range of state, local, and federal officials. That raises numerous privacy, security, and identity theft concerns.

Our Core Concerns

Real ID raises numerous concerns regarding privacy, fairness, cost, and practicality. However, the core privacy dangers with the legislation are:

- **An identity theft honeypot.** Access to the information contained on the Real ID cards and in the distributed Real ID database will be a valuable commodity eagerly sought by identity thieves. Under Real ID, drivers' licenses and database of motorist information will contain valuable information for an identity thief, including date of birth, social security number, gender, place of birth driver's license or identification card number, digital photograph, address, signature and a full copy of a driver's birth certificate. Identity thieves already recognize the value of motorist information and are increasingly targeting state Motor Vehicle Departments. Under Real ID, drivers' license information could be accessible from tens of thousands of locations across the country and contain even more valuable information.¹ If the personal information in the Real ID database is not protected, that system will be an active threat to individuals.
- **Private-sector piggybacking.** The mandated machine-readable technology makes it especially likely that private businesses will make use of the card's infrastructure to create a parallel, private database, one that will be outside the reach of the Privacy Act and contain much more information than government databases. Bars swiping licenses to collect personal data on customers may prove to be just the tip of the iceberg as every convenience store learns to grab that data and sell it to Choicepoint for a few pennies – building massive private sector files of personal information, all linked to an individual through their ID.

¹ For a survey of press reports documenting problems see Center for Democracy and Technology, "Unlicensed Fraud: How bribery and lax security at state motor vehicle offices nationwide lead to identity theft and illegal driver's licenses," January 2004, pp. 5-7

- **Expanded government use.** The Real ID and the database behind it has the potential to become a tool for not only verifying identity but also for:
 - Tracking movement through the preservation of data on the place and time of ID checks
 - Serving as the repository for an ever-expanding amount of data
 - Linking together disparate information currently scattered across different government databases

Protecting against identity theft and preserving privacy means safeguarding information in two key areas: on the card itself, especially the machine-readable component and in the database

Specific Implementation Questions That DHS Is Facing

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

While Congress has set the parameters of the law and provided guidance, the details of implementing the Real ID Act have been left to DHS. As the Agency promulgates regulations around Real ID it will be confronted with a series of questions whose answers will either protect or harm civil liberties and the privacy of Americans.

What type of machine readable technology will be used?

The Act is silent on the type of machine readable technology, such as a bar code or magnetic stripe, that will be used in licenses. One form of technology deserves particular mention: Radio Frequency Identification Chips. RFIDs pose particular privacy concerns because they can be read remotely without the bearer's knowledge or consent, and can be used to monitor an individual's movements.

Will the information on the card be secured?

Deciding whether to secure the Real ID information through encryption or some other means is a core privacy concern. If access is open and unlimited, the card would be more vulnerable to use and misuse for identity theft, data aggregation, or other purposes we haven't even imagined. A decision not to impose any kind of security mechanism will seriously limit the ability of DHS and the states to create other consumer and civil liberties protections around the card.

Who will have access to the machine-readable component and for what purpose?

As noted above, the information on the machine-readable component has the potential to harm individual privacy by creating an infrastructure for the tracking of consumer buying habits or creating a de facto internal US passport that tracks an individual's travel. However, with its proposed regulations DHS is in a position to curb misuse of the Real ID while still maintaining its value as an identity document. For instance, DHS could create a layered system (or

at least create standards that lay the groundwork for the creation of such a system by the states) in which various actors could, depending on their purpose, verify the authenticity of the card, electronically read the card solely to determine if someone is of drinking age, to verify their name or other basic information, or access all the information on the card.

How are states going to gain access to the information contained in the motor vehicle databases of other states?

The Real ID Act could authorize the creation of one of the most comprehensive and far-reaching databases in American history. But the implementing regulations could control the dissemination of potentially sensitive information, such as address or photographs, and could limit who would have access to information. For example, DHS could create a system whereby one state's motor vehicle department would simply verify that an individual has a valid license in another state by receiving a binary yes/no answer, rather than having access to the other state's entire file on that individual. Such a system would protect the validity of licenses without unnecessarily sharing personal information.

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

What type of access will government actors have to the database?

Federal and state agencies will inevitably push to extend the Real ID database beyond its original purpose. Will the database be linked to other records (such as the National Crime Information Center (NCIC)) to become the backbone or index for individual profiles on every American? Will law enforcement be able to use the fingerprints or other biometrics that states collect as part of its criminal investigations? Will law enforcement or other government actors have to abide by any principals of proportionality where information is only released to the extent necessary to perform specific functions, and fishing expeditions are prohibited? DHS is now confronted with a decision over whether seeking an identity document authorizes a massive intrusion by the government into the lives of every American.

Will DHS leave the states any flexibility?

States have traditionally crafted careful protections around motor vehicle information, including how motor vehicle departments can disseminate the information, how that information can be used, and who can gain access to sensitive information like addresses.

The states have had to wrestle with a complex thicket of issues that may well lie outside of the institutional expertise of DHS. For example, the requirement that driver's licenses include a person's address raise issues such as whether exceptions can be created for people like criminal court judges, how homeless individuals are treated, and domestic violence victims. If DHS sweeps away the body of law that has grown up in the states to deal with this and many other complexities, it could not only create numerous practical and political

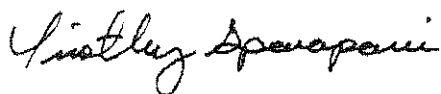
problems, but also create an enormous and unnecessary loss of privacy for every American.

As you have sought to draft regulations, the practical dilemmas posed by Real ID have no doubt provided daunting.

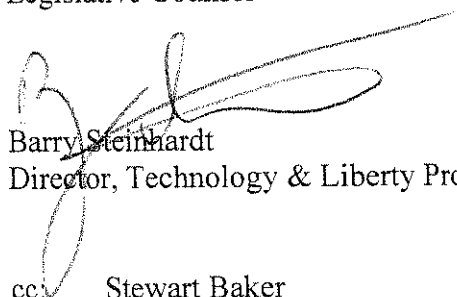
If your experience has convinced you that the statute does not allow Real ID to be implemented in a way that is practical or fair, we hope you will join with the growing chorus of state officials and advocates that have called for the Real ID Act to be revisited.

Sincerely,

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION



Tim Sparapani
Legislative Counsel



Barry Steinhardt
Director, Technology & Liberty Project

cc. Stewart Baker
Assistant Secretary for Policy

Jonathan Frankel
Director of Law Enforcement and Information-Sharing Policy