Electronic Frontier Foundation and World Privacy Forum comments to DHS on REAL ID Act regulations, DHS-2006-0030

May 8, 2007

The Electronic Frontier Foundation (EFF) and the World Privacy Forum (WPF) respectfully submit these comments on the Department of Homeland Security's (DHS) proposed REAL ID Act regulations, *Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, Docket No. DHS-2006-0030.

The Act is profoundly flawed on a number of levels, and the regulations implementing the Act cannot escape these flaws. The states apparently agree: "seven states have enacted statutes or resolutions opposing the implementation of Real ID, and Oklahoma is on the verge of becoming the eighth. Oklahoma City and Tulsa aren't known as liberal hotbeds. Anti-Real ID measures have passed at least one chamber of legislatures in 14 states and been introduced in 11 others." "Real ID Revolt," *The Wall Street Journal* A18 (May 8, 2007), available at http://online.wsj.com/article/SB117858856442095301.html (Real ID Revolt).

Most important, the Act creates a national identification (ID) card that will become a practical necessity for anyone wishing to travel on an airplane, open a bank account, collect Social Security payments, or take advantage of nearly any government service, including health care. As one privacy expert has said, "These new REAL ID-compliant cards will probably become de facto national ID cards." A. Michael Froomkin, *Creating a Viral Privacy Standard*, 48 Boston Coll. L. Rev. 55, 81 (2007). Both the DHS Notice of Proposed Rulemaking (NPRM) and the DHS Privacy Impact Assessment (PIA), DHS Privacy Office, *Privacy Impact Assessment for the REAL ID Act* (Mar. 1, 2007) <http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realid.pdf >) struggle to show that the REAL ID will not be a national ID card, but their efforts are unconvincing.

Further, beyond being a deeply flawed national ID system, the Act and its regulations omit crucial privacy and security protections to the point that the NPRM directly conflicts with privacy and security principles that the U.S. government has twice ratified, and which Congress expressly referenced in the Act and its legislative history.

EFF and WPF urge DHS to withdraw these proposed regulations in their entirety. We further urge DHS to ask Congress to suspend implementation of the REAL ID Act, and to hold legislative hearings to investigate how to repair the REAL ID. Identification policy is far too important and complex to be a matter of task force recommendations or political rhetoric, negotiation, and compromise. While the Akaka-Sununu bill is a significant improvement over the REAL ID status quo, it is not substitute for public debate about national ID systems.

Statutory background

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. No. 108-458, empowered the Secretary of Transportation, in consultation with the Secretary of Homeland Security, to issue regulations with respect to minimum standards for federal acceptance of driver's licenses and personal identification cards. IRTPA required that the

Secretary issue regulations within 18 months of enactment that require each driver's license or identification card, to be accepted for any official purpose by a federal agency, to include the individual's: (1) full legal name; (2) date of birth; (3) gender; (4) driver's license or identification card number; (5) digital photograph; (6) address; and (7) signature. In addition, the cards must contain physical security features designed to prevent tampering, counterfeiting or duplication for fraudulent purposes; as well as a common machine-readable technology with defined minimum elements.

Even after IRTPA's enactment, the states retained considerable discretion in issuing driver's licenses. While IRTPA specified that federal regulations include minimum standards for the documentation required by the applicant, the procedures utilized for verifying the documents used, and the standards for processing the applications, the regulations were prohibited from infringing upon a state's power to set criteria concerning what categories of individuals are eligible to obtain a driver's license or personal identification card from that state and from requiring a state to take an action that conflicts with or otherwise interferes with the full enforcement of state criteria concerning the categories of individuals that are eligible to obtain a driver's license or personal ID card.

In short, IRTPA did not authorize the federal government to restrict a state's power to decide *who* may be eligible for a driver's license (e.g., aliens, legal or illegal). In addition, IRTPA:

- did not require uniform design of driver's licenses;
- required procedures to protect the privacy rights of individual applicants;
- required negotiated rulemaking under the Administrative Procedure Act, including representatives from: (1) state and local offices that issue drivers' licenses and/or personal identification cards; (2) state elected officials; (3) Department of Homeland Security; and (4) interested parties.

The REAL ID Act of 2005 set up a national standard for the issuance of state driver's licenses. REAL ID Act of 2005, Pub. L. No. 109-13, div. B, 119 Stat. 231, 302. Title II of REAL ID, "Improved Security for Drivers' Licenses and Personal Identification Cards," lays out requirements for new state ID cards. See div. B, tit. II, 119 Stat. at 311 (codified at 49 U.S.C.A. § 30301 note (2006)).

Unlike IRTPA, the REAL ID Act effectively preempted all state and local laws and regulations regarding driver's licenses in favor of national statutory standards and forthcoming corresponding regulations, and repealed all provisions of IRTPA inconsistent with national standards. It also repealed the IRTPA requirement of negotiated rulemaking and procedures to protect the privacy rights of individual applicants.

Under REAL ID, starting on May 11, 2008, "a Federal agency may not accept, for any official purpose, a driver's license or identification card issued by a State to any person unless" that state credential complies with technical standards issued by DHS. Id. § 202(a). The DHS Secretary may extend this deadline. Id. § 205(b).

REAL ID requires that states comply with extensive rules about how they issue driver's licenses, and defines in some detail what information those licenses must contain. See

REAL ID Act of 2005, § 202(b)–(d). The license must contain the holder's actual residence addresses (rather than a post office box), full legal name, birth date, gender, signature, and driver's license number, and a digital photograph of the person's face. Id. § 202(b), (d)(3).

Before issuing a driver's license that will qualify as valid under REAL ID, the states must require and verify the applicant's documentation, id. § 202(c)(1), (d)(4), either a photo ID document or a non-photo ID document that contains both the applicant's full legal name and date of birth. Id. § 202(c)(1)(A). States must verify the applicant's name, primary address, date of birth and SSN (or proof of Social Security ineligibility). Id. § 202(c)(1)(B)–(D). Indeed, states must verify "with the issuing agency" the issuance, validity, and completeness of *each document* required to be presented by the person. Id. § 202(c)(3)(A) (emphasis added).

States may not accept any foreign document other than an official passport. Id. § 202(c)(3)(B). States can only issue driver's licenses to citizens, permanent residents, certain asylum seekers, and the holders of particular types of visas. Id. § 202(c)(2)(B). The list of visa classes that qualify for a driver's license is noticeably shorter than the list of visa types that permit long-term residence and even employment in the United States. See 8 C.F.R. §§ 204, 205, 212, 214, 244 (2006).

The card must include physical security features (as defined by the DHS regulations), designed to prevent tampering, counterfeiting, or duplication. Id. § 202(b)(8); see id. § 205(a), 119 Stat. at 315 (granting the DHS Secretary authority to issue regulations under REAL ID).

REAL ID also tries to ensure that driver's licenses will be unique. If a person presents an out-of-state driver's license as ID, the issuing state must confirm that the out-of-state license is being terminated before issuing a new one. Id. § 202(d)(6).

REAL ID specifies that licenses will have to be machine-readable by a "common machine-readable technology." Id. § 202(b)(9).

Last but not least, the REAL ID Act establishes a system of databases. Each state must maintain a state motor vehicle database that contains: (A) all data fields printed on driver's licenses and IDs issued by the state; and (B) motor vehicle drivers' histories, including motor vehicle violations, suspensions, and points on license. Id. § 202(d)(13). This database must be shared with other states. Id. § 202(d)(12). Also, states must retain digital images of identity source documents in electronic storage in a transferable format, id. § 202(d)(1); they must retain paper copies of source documents for a minimum of seven years or images of source documents for a minimum of ten years, id. § 202(d)(2).

The Fair Information Principles and their Relationship to DHS and REAL ID

The Fair Information Principles (FIPs) are a set of internationally recognized privacy protection principles initially proposed by a U.S. government advisory committee in 1973 (HEW report, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*). In 1980, the Organization for Economic Cooperation and Development (OECD) published a revised set of principles. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. The eight 1980 FIPs have been widely adopted, and are viewed by the

U.S. Government Accountability Office as the basis of the Privacy Act and as the bedrock of the privacy standards by which U.S. government agencies assess, construct, and implement their actions.

DHS has expressly acknowledged the 1980 OECD Fair Information Practices and expressed the desirability of their application to U.S. government systems, including mixed systems. DHS Privacy Policy Guidance Memorandum 2007-1, at 3 (January 19, 2007).

Additionally, the OECD guidelines were an integral part of the U.S. Department of Justice Global Information Sharing Initiative's guidelines and guidance. U.S. Department of Justice, Global Information Sharing Initiative, Privacy Policy Development Guide at 33, 40, 73, 113 –116, 143, 145 (Sept. 2005).

The Fair Information Principles are the following:

- Openness

  There should be a general policy of openness about practices and policies with respect to personal information.

- Collection Limitation

  Personal information should be collected by lawful and fair means and only the information necessary for the stated purpose should be collected.

- Purpose Specification

  The purpose for collecting personal information should be specified at the time of collection. Further uses should be limited to those related to that purpose.

- Use Limitation

  Personal information should not be used for purposes other than those specified, except with the consent of the subject or by the authority of law.

- Data Quality

  Personal information should be accurate, complete, timely and relevant to the purpose for which it is to be used.

- Individual Participation

  Individuals should have the right to inspect and correct their personal information.

- Security Safeguards

  Personal information should be protected against such risks as loss, unauthorized access, destruction, modification or disclosure.

- Accountability

  An organization should be held accountable for compliance with the organization's privacy policies, and should provide redress for failure to comply with them.

Implementing these principles would protect the privacy of those whose personal information would be contained in REAL ID databases and systems. Each principle should be looked at and specifically implemented by DHS.

For example, the principles of Purpose Specification and Use Limitation require that the purpose for collecting the information be disclosed and that uses be limited to that purpose. In the case of REAL ID, the purpose should be limited to the "official purposes" enumerated in the Act and in the NPRM at § 37.03. Consistent with those principles is the use of encryption of the data in the machine-readable zone to prevent secondary use.

The principles of Individual Participation, Data Quality, and Accountability all underlie the need for a timely and robust redress procedure for individuals whose records contain errors, inaccuracies, or fraudulent information.

The Security principle requires limiting access to all databases containing personal information to those with an official enumerated need to know and only as required for the purpose of administration of DL/ID cards and for purposes enumerated in existing law.

I. The REAL ID Act and its regulations create a national ID system

REAL ID is a grave danger to civil liberties and privacy because it creates a national ID system. Even before REAL ID, it was well understood that a system of national ID not only poses a "wide range of technological and logistical challenges," but has "serious potential for infringing on the rights and freedoms of ordinary citizens." National Research Council, Computer Science and Telecommunications Board, Committee on Authentication Technologies and their Privacy Implications (hereinafter "NAS Committee"), IDs — NOT THAT EASY: QUESTIONS ABOUT NATIONWIDE IDENTITY SYSTEMS 47 (2002) (IDs— NOT THAT EASY).

DHS acknowledges that the REAL ID Act has been criticized for "creat[ing] a national identity card and centralized database on all drivers." NPRM, at 24. But its understanding of the problem is limited. "This concern stems from the provisions in the Act requiring that the individual States electronically verify application information against Federal databases and provide State-to-State access to verify that each applicant only holds a valid license in one jurisdiction." Id. DHS then defends the REAL ID system by saying: "the recommended architecture for implementing these data exchanges does not create a national database, because it leaves the decision of how to conduct the exchanges in the hands of the States." NPRM, at 25.

One pair of security experts recently explained: "While it's true that the system is not a single database per se, this is a semantic dodge; according to the DHS document, Real ID will be a collaborative data-interchange environment built from a series of interlinking systems operated and administered by the states. In other words, to the Department of Homeland Security, it's not a single database because it's not a single system. But the functionality of a single database remains intact under the guise of a federated data-interchange environment." Richard Forno and Bruce Schneier, *National ID card a disaster in the making*, http://news.com.com/2010-7348-6180835.html?tag=tb (May 3, 2007).

DHS unpersuasive defense shows that it either does not understand, or refuses to acknowledge, Americans' deep and wholly rational objections to national ID cards. U.S. "citizens' concerns for civil liberties, their historic association of ID cards with repressive

regimes, and states' rights concerns have discouraged movement toward a governmentally sanctioned nationwide identity system." IDs— NOT THAT EASY at 7.

The problem is not a card or even a national database. A national ID system is an entire system of databases, information gathering activities, and human beings making fateful judgments about individuals based on that overall system. The standardized national driver's licenses created by REAL ID would become a key part of a system of identity papers, databases, status and identity checks and access control points - an "internal passport" that will increasingly be used to track and control individuals' movements and activities. Such a system not only infringes privacy but the rights of free speech, association, and travel. *E.g., Shapiro v. Thompson*, 394 U.S. 618, 629–31 (1969) (recognizing a constitutional right to interstate travel).

Further, we question the overall architectural integrity of the system that has been proposed. Where are the neutral third-party studies and documentation that definitively prove that this system, as enacted and as planned, will work, and will work to actually improve security in a cost-effective manner? The ideas behind the REAL ID Act were subject neither to vigorous public debate nor to vigorous independent scientific review.

Unfortunately, the costs of a national ID system exist regardless of whether the system actually protects against terrorists. A national ID system is likely to be the worst of both worlds — dangerous to a free society without making us any safer. This is a bad bargain.

DHS argues that a de facto national ID system is already in place, and that the agency is only making existing driver's licenses more secure. Current practice does not substantiate this argument. How often do individuals have their driver's license swiped in a card reader, which is linked back to a central government database or set of databases?

"Given the wide range of technological and logistical challenges, the likely direct and indirect costs, the serious potential for infringing on the rights and freedoms of ordinary citizens, and the gravity of the policy issues raised, any proposed nationwide identity system requires strict scrutiny and significant deliberation well in advance of design and deployment." IDs— NOT THAT EASY, at 47. Simply put, a national ID card is a commitment to a system of massive social surveillance that is alien to our constitutional tradition.

The card and its ID number will be a "super-identifier"

Obviously, we use many ID cards in America today. But these ID cards – driver's licenses, credit cards, employee badges, and so on – are issued and used for limited purposes under decentralized governance. Major companies do aggregate such data about us, but the overall system is not under government control.

Converting from a system of many similar cards to a mandatory governmental system of uniform cards is a major change.

"A nationwide identity system . . . might drive many other forms of identification out of use by subsuming their functionality. Several factors in particular could encourage widespread third-party reliance on the nationwide identity system to the exclusion of current systems. First, if the cost of the system is borne by the government and its associated agencies, the system's use would be free to other segments of society unless measures (technical, legal, or otherwise) are taken to prevent unauthorized use. Second,

unless private parties are prevented by law (or restrictions on technology) from relying on the nationwide identity system, the liability associated with such reliance would be shielded by the government's sovereign immunity. Third, even if the private parties were forbidden to rely on the data, it is very likely that private commercial organizations would begin to correlate data about citizens based on their card and/or identity within the system." IDS—NOT THAT EASY, at 30–31.

As a result, the REAL ID number may well become a "super-identifier" that acts as a key to tie address, name, and Social Security Number (SSN) together with a biometric. The REAL ID number will become a primary authenticator of identity in many transactions. Like SSNs, REAL ID numbers would be widely known and therefore susceptible to use by identity thieves.

The DHS Privacy Office, to its credit, forthrightly admits this problem. "All identity systems trigger privacy concerns and extend not only to the use of a credential, but to the use of any unique number associated with the credential. . . . This is a risk inherent to the law enacted by Congress and the proposed implementing regulations cannot ameliorate this risk." PIA, at 6. We agree, and we also agree that if REAL ID were to continue, the unique ID number should not be in the MRZ. PIA, at 17.

Checkpoints and databases run amok

The card and its number are only the tip of the national ID surveillance iceberg. Not having data collected about you obviously protects privacy. Conversely, a crucial and obvious dynamic associated with national ID cards is more ID checking and more gathering of information about who does what where. As discussed above, the REAL ID will become a standard for both the private and the public sector, and all of the associated data will be linked to a single standard super-SSN.

This is a serious privacy problem. "[H]istorically, totalitarian governments have developed elaborate systems for collecting data about people's private lives." Daniel Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S.Cal. L. Rev. 1083, 1102 (2002); Pamela Samuelson, *Privacy as Intellectual Property*, 52 Stan. L. Rev. 1125, 1143 (2000) ("One factor that enabled the Nazis to efficiently round up, transport, and seize assets of Jews (and others they viewed as 'undesirables') was the extensive repositories of personal data available not only from the public sector but also from private sector sources.").

Under REAL ID, every state's DMV database will be linked and much personal information – from SSNs and birth dates to copies of birth certificates and bank statements – will be accessible to many people across the country.

The machine readability of the REAL ID card will exacerbate the privacy problem. The requirement of a uniform technical standard (2D barcode) for the machine-readable zone on the REAL ID card and the requirement that such zone contain personally identifying information (§ 37.19) would accelerate the transformation of state-issued driver's licenses into national ID cards. As the DHS PIA recognizes, the requirement of a uniform technical standard for the MRZ on the REAL ID DL/IDs of all states would reduce the cost of scanning equipment, thereby increasing the likelihood of secondary uses by private sector and governmental entities. In addition, the inclusion of the personally

identifying information from the front of the card in the machine-readable zone also facilitates the creation of databases for secondary uses. PIA, at 14. We agree with the DHS Privacy Office that "Neither the Act nor the House Conference Report support harvesting the information from the MRZ on the credentials." Id., at 15. DHS should have implemented regulations making it unlawful for third parties to harvest data from the MRZ. We do not understand why the DHS Privacy Office believes that DHS lacks the authority to do so. Id., at 14.

Also, requiring states to maintain databases of foundational identity documents will also create an incredibly attractive target to criminal organizations, hackers, and other wrongdoers. The breach of a state's entire database, containing copies of birth certificates and various other documents and information, could topple the identity system we use in the United States today. The best data security is not creating large databases of sensitive and valuable information in the first place.

Meanwhile, the requirement that states make their databases available to every other state exposes each state to the security weaknesses of all the others. There is no way to ameliorate all the consequences of the REAL ID Act requirement that information about every American driver be made available to every other state.

Because Congress did not clearly define the purposes of the REAL ID Act, its national ID system will suffer from severe mission creep

Among the basic privacy principles (FIPs) are Purpose Specification, requiring collectors of personally identifying information to inform individuals of the purposes for which they are collecting it at the time of collection, and Use Limitation, requiring data owners to limit their use of personally identifying information to the purposes originally specified. DHS has a responsibility to implement the full standard of FIPs.

The "official purposes" of a REAL ID, as provided in the Act and in the NPRM at § 37.03, are: accessing Federal facilities, boarding Federally regulated commercial aircraft, and entering nuclear power plants. Because these are the only "official purposes" for the REAL ID, apart from driving, these purposes must be specified to applicants at issuance – and no other purposes can be allowed.

Unfortunately, the Act contemplates multiple uses for the REAL ID, and acknowledges that the activities associated with the REAL ID will likely expand greatly. The NPRM correctly states:

> The rule would give states, local governments, or private sector entities an option to choose to require the use of REAL IDs for activities beyond the official purposes defined in this regulation. To the extent that states, local governments, and private sector entities make this choice, the rule may facilitate processes which depend on licenses and cards for identification and may benefit from the enhanced security procedures and characteristics put in place as a result of this proposed rule.

NPRM, at 108. The DHS thus acknowledges that REAL ID facilitates function creep and creates a serious concern that private parties such as insurance companies, educational institutions or employers, will use REAL ID licenses for identity verification and other purposes.

Massed personal information will be an irresistible attraction to the Department of Homeland Security and many other governmental entities, all of which will dip into the data for an endless variety of purposes. As Anne Collins, the Registrar of Motor Vehicles for the Commonwealth of Massachusetts recently told DHS's Data Privacy and Integrity Advisory Committee: "If you build it they will come."

The REAL ID database will inevitably become the repository for more and more data on individuals, and will be drawn upon for an ever-wider set of purposes. Its standardized machine-readable interface will drive its integration into an ever-growing network of identity checks and access control points each of which will create new data trails that will in turn be linked to that central database or its private-sector shadow equivalent.

The DHS Privacy Office correctly notes: "The only way to prevent misuse of any identifier is to establish enforceable restrictions at the time any REAL ID identifier is introduced." PIA, at 7. Yet neither the REAL ID Act nor the proposed DHS regulations even attempt to control mission creep.

While the proposed regulations do not add to the Act's list of "official purposes," they indicate that DHS will consider expanding the list in future proceedings, including controlling "unlawful employment," gun ownership, drinking, and smoking. NPRM, at 109. Clearly, the government anticipates expanding the functions of REAL ID once this particular regulatory hurdle is overcome.

The REAL ID national ID system will not be effective against terrorism.

REAL ID was enacted to protect against terrorism. NPRM, at 108. But identity-based security aimed at Americans is not an effective way to stop terrorism. "The terrorist attacks of September 11, 2001, were carried out exclusively by non-U.S. nationals; none of them would have had a U.S. ID if one had been required only of citizens. In addition, undercover operatives sponsored by a major foreign group or state hostile to the United States generally are individuals without suspicious records. It follows that such people's IDs (be they within a United States nationwide identity system or outside it) would not contain anything particularly problematic." IDs – NOT THAT EASY, at 20 n. 7.

Moreover, determined foreign terrorists will always be able to obtain fraudulent documents (either counterfeit or real documents bought from corrupt officials). "As an example of this, the Washington Post reported that 15 of the September 11 hijackers applied for visas in Saudi Arabia, where officials have indicated that identity theft is a serious concern." IDs – NOT THAT EASY, at 20 n. 10, citing <http://www.washingtonpost.com/wp-dyn/articles/A14788-2001Oct30.html>.

Indeed, DHS correctly admits that we cannot easily verify foreign credentials. NPRM, at 53 ("verifying the foreign passport itself with the Government that issued it is simply not feasible"). As the NAS Committee explained:

"Even if IDs were issued to foreign visitors entering the United States, the information would be based on information provided by their country of origin. Its usefulness is limited for at least two reasons: (1) many countries do not have much data about their citizens to begin with, and others may be unlikely to provide other nations with suspicious background information about their own citizens and (2) even if a country indicates that an individual seeking admission to the United States has a problematic

background record, that doesn't mean the United States would consider such a person a risk (for example, a country might provide warnings about political dissidents). Adding information to an individual's ID beyond what his or her country of origin provides (presumably gathered by U.S. intelligence) is problematic for a number of reasons, including cost, scale, paucity of data, and potential compromise of sources and methods behind the information." IDS – NOT THAT EASY, at 20 n. 9.

Thus, the brunt of REAL ID falls on ordinary Americans, who are even less likely to be terrorists.

More fundamentally, ID system proponents seem to think that the security problem lies in being unable to verify identity. But ID documents do not reveal anything about what the identified person is likely to do; thus, "[m]uch of the utility of the national ID card assumes a pre-existing database of bad guys. We have no such database." Bruce Schneier, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD 205 (2003).

Because no such database exists, a national ID system entails a powerful commitment to widespread social surveillance in order to try to identify "bad guys" – to distinguish the suspicious from the ordinary. We already know of such databases, watch lists, and other forms of generalized social surveillance, like "Terrorist Information Awareness" and "Secure Flight." These programs are not only generally hostile to privacy, free speech and other civil liberties but create specific risks such as "hasty judgment in times of crisis, the disparate impact of law enforcement on particular minorities, cover-ups, petty retaliation for criticism, blackmail, framing, sweeping and disruptive investigations, racial, ethnic, or religious profiling, and so on." Solove, *Digital Dossiers*, at 1104. And the combination of bureaucratic opacity and official secrecy that surrounds these systems have created arbitrary and capricious government regulation and enforcement behavior that both defies and undermines the accountability that the rule of law and our constitutional system requires.

The REAL ID system will not prevent identity theft

It appears that no part of the REAL ID system has been risk-mitigated specifically against ID theft. For example, there is not a specific security plan in place to mitigate theft and misuse of the foundational identity documents housed in multiple locations. Further, there is no plan to address security of the resulting information that will be disseminated to thousands of terminals and devices across the nation, accessible by DMV employees and others.

If any foundational document is compromised or if any of the systems are tampered with or breached, then the REAL ID will simply be a hardened ID that will make it more difficult for an individual to get corrected.

Moreover, because a physical ID is not needed to commit identity theft, the swiping and abuse of the machine readable information on the card can facilitate repositories of mass data stores of identity information that will be invaluable to thieves. Bad actors can and will get access to employment that allows them to scan REAL IDs. This poses identity theft problems. For example, the Department of Justice and the Federal Trade Commission discuss medical identity theft in their 2007 *President's Identity Theft Task*

Force Strategic Plan. Today, medical identity theft occurs when harvested information is used to access hospitals for health care, as in *United States v. Sample*, 213 F.3d 1029 (8th Cir. 2000). REAL ID stands to facilitate and exacerbate this problem precisely because machine readability will make harvesting easier.

II. The contemplated REAL ID system imposes astronomical financial costs

Before the passage of the REAL ID Act, the Congressional Budget Office had estimated that its costs would be around $100 million. Critics derided this estimate as laughably low, and in September 2006 the National Conference of State Legislatures estimated that REAL ID would cost about $11 billion over the first five years.

But even these numbers are low, according to DHS, which estimates that REAL ID will cost the states and individuals from $17.2 billion to $23.1 billion over 10 years. NPRM, at 106. And there is no guarantee that these numbers are accurate; in fact, there is every reason to believe that they are low given that DHS has no clear idea of how to implement the REAL ID Act's dictates – and has made some unrealistic calculations.

For instance, DHS estimates that individuals' DMV visits will have a marginal cost of 64.7 million hours. NPRM, at 106. But this number must be spread over the 240 million driver's license holders. Simple arithmetic tells us that DHS expects REAL ID to add about 15 minutes to the average DMV visit. This number is unrealistic. As the Wall Street Journal sarcastically noted: "In California today, where a nation-high 25 million licenses are issued, residents can renew by mail. Real ID requires that you appear in person. So Americans can be grateful that DMVs nationwide are known as models of hassle-free efficiency; be sure to book a free afternoon." Real ID Revolt; see discussion below at p. 14.

Yet no provisions were made to pay for implementation of the Act or to streamline the administrative burdens on states and individuals. Slowing implementation, as some have suggested, see Nat'l Governors Ass'n et al., The REAL ID Act: National Impact Analysis 2 (2006), available at http://www.nga.org/Files/pdf/ 0609REALID.pdf, is no answer because the Act itself is fundamentally flawed.

III. The DHS REAL ID Regulations are unrealistic, unworkable, and excessively burdensome

Even if the REAL ID system were not an enormous danger to civil liberties, it is fatally flawed because it demands the impossible or near impossible from the states. Many of the problems are posed by the Act's identity and document verification requirements.

DHS's document verification requirements are onerous

Driver's license applicants must submit to the DMV proof of citizenship, a birth certificate and two proofs of address to acquire and renew a REAL ID. DHS Regs § 37.11.

States must then verify with the issuing agency the issuance, validity, and completeness of these documents. § 37.13.

1. States must verify birth certificates through the Electronic Verification of Vital Events (EVVE) System, or an alternative approved by DHS.

2. States must verify a U.S. passport or Consular report of birth abroad through existing State Department systems.

3. States must verify documents demonstrating permanent residence through the Systematic Alien Verification for Entitlements (SAVE) system, or an alternative approved by DHS.

4. States must verify DL/ID cards with the state of issuance.

5. States must verify SSNs with the SSA's electronic database.

6. States must verify documents demonstrating address of principal residence in accordance with "a system of document verification acceptable to DHS."

The requirement that states verify applicants' documents with their sources is one of the Act's critical components, intended to increase the integrity of the REAL ID DL/ID card as an identification document. DHS states that the verification "will increase security by reducing the ability to fraudulently manufacture documentation typically used to obtain driver's licenses and identification cards." NPRM, at 47-48.

Common sense alone tells us that the Act's burdens on the states (and on individuals) are staggering. But DHS has dodged these implementation problems, despite considerable delay in the promulgation of the NPRM, by pinning its hopes on "vaporware systems" that do not exist or have not been tested on a national scale and likely will not exist or be tested for a long time.

As the National Governors Association recently told Congress,

"The proposed regulations identify five systems that will be required to make Real ID work: Social Security On-Line Verification (SSOLV), Electronic Verification of Vital Events Records (EVVER), Systematic Alien Verification for Entitlements (SAVE), an all-drivers system run by the states to ensure an applicant is not licensed in another state and a system run by the U.S. State Department to verify foreign passport information. *Only SSOLV is fully operational on a national basis and even it will require enhancements to handle the volume anticipated under Real ID. The other systems are either not widely used, in the developmental or pilot phase, or do not exist."*

Statement of David Quam, Director, Federal Relations, National Governors Association, Before the Subcommittee on Oversight of Government Management, the Federal Workforce and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate, *Understanding the Realities of Real ID: A Review of Efforts to Secure Drivers' Licenses and Identification Cards* (March 26, 2007) (emphasis added), http://www.nga.org/Files/pdf/0703STATEMENTREALIDQUAM.PDF.

In short, any hoped-for improved security and integrity cannot be achieved because no mechanisms truly exist for implementing REAL ID.

DHS is apparently aware of these problems. For instance, the Act clearly requires that states verify "address of principal residence" with the "issuing agency" of such documents. Act, § 202(c)(3)(A). But nothing in the Act or the regulations addresses the duties of such "issuing agencies," e.g. utility companies, to assist the state in verifying residence address. Thus, as DHS concedes, "there is no nationally available, reliable, up-to-date, and cost-effective method for States to verify this information with the issuing

source of the document, as the plain language of the Act would seem to require." NPRM, at 48-49.

DHS thus concedes that the Act's unrealistic standards cannot be met, and sets a vague requirement that documents be presented and accepted under a policy acceptable to DHS. NPRM, at 50. Nevertheless, address verification is required by § 37.11 (f) (1), (2), (3) (p. 134); § 37.13 (a) (6) (p. 137). Yet as security experts Forno and Schneier note, "while the department concedes it's a monumental task to prove one's domicile or residence, it leaves it up to the states to determine what documents would be adequate proof of residence--and even suggests that a utility bill or bank statement might be appropriate documentation. If so, a person could easily generate multiple proof-of-residence documents. Basing Real ID on such easy-to-forge documents obviates a large portion of what Real ID is supposed to accomplish." , http://news.com.com/2010-7348-6180835.html?tag=tb

Here, as elsewhere, the true problem is that Congress asked for the impossible.

Similarly, DHS recognizes enormous problems with the verification of other identity information. The EVVER system "has not been tested nationwide," but "such a system *could* be in place and fully operational by May 2008." NPRM, at 51 (emphasis added). But nothing in the NPRM indicates that this is likely to actually happen, and DHS admits that persons born before 1935 are unlikely even to have birth certificates. "It is anticipated" that there will be electronic verification of U.S. passports, NPRM, at 52, but this again appears to be wishful thinking.

Moreover, whether or not the systems themselves exist, "each State must have electronic access" to such databases, because "[s]ecure and timely access to trusted data sources is a *prerequisite* for effective verification of applicant data." NPRM, at 57 (emphasis added).

Sharing information in state databases with all other states is one of the most difficult challenges of Real ID. It is DHS's "highest priority"; "DHS will work closely with the States"; "DHS will provide assistance to states"; "DHS will actively support" and so on. See generally NPRM, at 57-62. But this connectivity problem remains unsolved. In essence, DHS abdicates responsibility and leaves it to the states to figure it out.

DHS states that it plans to build upon the existing infrastructure of Federal statutes, regulations and data systems (i.e., Commercial Driver License Information System (CDLIS) and National Driver Register/Problem Driver Pointer System (NDR/PDPS) in implementing REAL ID and will work closely with the Department of Transportation, AAMVA and the States to fulfill the requirements for State-to-State data exchange. NPRM, at 61. But this system is also vaporware.

The "prerequisite" connectivity does not exist, and DHS only promises to help the states. Again, Congress is to blame; DHS cannot do the impossible. But neither can the states, and DHS has now proven that almost two years of regulatory drafting cannot change reality. It is hardly surprising that the states are fed up with REAL ID.

Acknowledging reality, DHS comments that verification "may be phased in over time" (NPRM, p. 47). More time is no answer. States should not be required to start implementing the Act until the necessary systems and tools for verifying applicants' document at issuance actually exist and have been shown to work efficiently enough to

permit compliant issuance. This includes systems for verifying birth certificates and DL/IDs of all jurisdictions. Nor can states possibly develop the required security plans without good knowledge of how these systems work in practice. It is absurd to ask the states to try to comply with ever-shifting compliance targets. Until these are systems are actually implemented, states cannot reasonably comply with the proposed rules.

Other burdens on the states are similarly onerous

Because the states vary greatly in their driver's license laws, they must adopt conforming legislation and honor procurement processes to implement the Act's far-reaching changes. Independently of harm to individuals themselves, the states will be massively burdened.

Most important, the Act will require major efforts in storing and transferring data. The California DMV's computer system, unfortunately, is old and difficult to upgrade. It uses about 1200 distinct computer programs, 70 percent of which were created in the 1960s using now-obsolete programming languages. Furthermore, about half of the current IT staff, which possesses the institutional knowledge about the systems and their underlying technologies, will be eligible to retire within a few years.

Address of principal residence: The DL/ID card currently displays an address. California allows for the display of a P.O. Box on the card, however a physical address is required to be submitted and retained on their DL record for legal purposes.

Individuals qualifying for confidentiality may have their residence address blocked from the record. California, like many states, has laws that protect the safety of certain groups of individuals by making their residential address confidential, including not requiring that it be displayed on their DL/ID card. Protected groups include law enforcement officers, judges, public officials, and victims of domestic violence.

Although § 37.17(f) excepts individuals enrolled in "State address confidentiality programs" and individuals whose addresses are entitled to be "suppressed" under state or federal law from the requirement to display address of principal residence on the DL/ID card, this exemption is inadequate. Such "confidentiality programs" are limited to victims of domestic violence and those in related situations (e.g., stalking). In California, for example, other persons are not protected by "suppression"; they are protected by an address confidentiality program.

States are also required to use digital technology to electronically capture identity source documents. §37.31 (a)(b)(c) (p. 148). The Act and §37.31 of the proposed regulations require states to collect and maintain vast amounts of personally identifying information that they do not now maintain, including source documents such as birth certificates issued by numerous jurisdictions, immigration documents, documents containing Social Security numbers, and potentially utility bills and tax records. For California, in addition to significant costs for scanning equipment for 168 field offices, and the computer hardware and software necessary to capture, store and retrieve the documents, the new database of sensitive personal information represents a significant privacy and security risk.

Loss of virtual transactions: The population of California increases by more than 500,000 people per year, and much of that population growth occurs in geographic areas not

served by a DMV field office. One of the California DMV's most promising strategies for handling this growth, reducing congestion at DMV offices, and improving service to citizens is to promote the use of "virtual" transactions over the Internet. But the Internet could not be used for any REAL ID issuances, increasing the burden on the field offices.

Renewals: This problem also complicates renewals. DHS is also requiring states to limit the validity period of all non-temporary DL/IDs to less than 8 years. §37.21(b)(2) (p. 145). This will have a major impact on states that allow driver's licenses to be renewed without a physical visit to a DMV office. California, for instance, allows drivers with good records to renew their licenses by mail or over the Internet for up to two renewal cycles; California drivers with a "clean" driving record can go as long as 15 years before they must appear in-person at a DMV field office to renew the license. California also offers its senior citizens an identification card that is valid for ten years. The Act's eight-year limit will eliminate these programs and bring literally millions of additional applicants into California DMV offices earlier than required under current law, with staggering impacts on both the DMV and individual drivers.

Redress burdens: Problems are bound to occur in the complex submission, verification and issuance process mandated by the Act. Inevitably, persons will be unable to obtain REAL IDs for various reasons: lack of access to needed identity documents; verification problems because they were victims of identity theft or because of bad data in databases; simple error on the part of the DMV; and so on. In any such situation, an individual applying for a REAL ID will expect the state DMV to assist the individual in resolving the problem.

The challenge of correcting inaccurate records and providing appropriate redress for individuals is exacerbated by the distributed system and multiple sources of records required by REAL ID. The ability to correct errors in one's data is essential, since accuracy of information is the key to the effectiveness of REAL ID as an authoritative and reliable verifier of identity. Along with the correction of inaccurate data, the system must be able to facilitate routine updates, such as change of name or address, and to propagate them to all databases and systems where the data resides. When problems arise in the widely distributed systems for implementing the REAL ID Act, whether as the result of technology failures, human error, identity theft, or other forms of fraud, determining accountability will be very difficult. The lack of a multi-state governance structure would make it nearly impossible to correct errors in records and systems and propagate such corrections throughout a myriad of systems.

REAL ID imposes profound burdens on individuals as well

The burdens that REAL ID places upon individuals are profound and varied. Impacts range from discrimination to health care to cost to stalking.

REAL ID imposes multiple types of burdens on individuals

Because the federal government has appropriated only a small fraction of the necessary costs to implement REAL ID, the driver must bear the burden of higher costs at the DMV. DHS estimates that drivers will bear about 30% of the costs of REAL ID, optimistically believed to be more than $20 billion over ten years.

But such costs are only the tip of the iceberg. Like the states, individuals will be burdened by the Act's onerous documentation and verification demands, which require proof of citizenship, birth certificate and two proofs of address to acquire and renew a REAL ID. The DMV must then verify that these documents are authentic. This requirement will be particularly difficult for:

- Senior citizens
- Native Americans
- Victims of natural disasters like Hurricane Katrina
- Naturalized citizens
- Victims of domestic violence
- Immigrants
- People who live in RVs or are homeless.

The requirement that a REAL ID will be needed to enter federal facilities will have particularly unfair impacts. The very people who may have the greatest difficulty complying with the Act by providing verification documents - the poor, lawful immigrants, refugees, elderly people, and transient or homeless people - may also be most in need of the benefits and services offered at federal facilities.

Moreover, drivers will suffer horribly because DMV locations will be completely overburdened.

- Lines will be longer because it will take more time to process applications
- Mail and Internet renewals will have to be suspended.
- Individuals will have to wade through new bureaucracy in order to provide all the necessary documentation and make sure that their information is correct in multiple federal databases.

Women and others can be stalked using REAL ID cards and nationally linked databases

Requiring that individuals must allow their home addresses to be printed on the REAL ID card poses onerous burdens for many individuals. Unfortunately, because the REAL ID in effect publishes home addresses for individuals who are not protected in some way recognized by the NPRM – which excludes many people entitled to address confidentiality or suppression by states like California, see above at p. 14. the NPRM effectively gives stalkers the information they need to locate their targets. As the REAL ID becomes more widely deployed and required due to the lack of controls on the use of the card, scanning REAL IDs will likely become ubiquitous. Once this happens, mass lists of names, home addresses, and other information will be even easier to assemble, sell, and trade.

Individuals who fall into a protected category in REAL ID will perversely stand out to those asking to see ID cards because they have a PO Box or alternate address on their REAL ID cards.

As the use of the REAL ID expands, the way home addresses are being handled on REAL ID cards stands to contribute to serious public safety issues both for those who

have a protected status, and those who do not. DHS needs to take these issues back to the table and specifically allow women and others to proactively protect themselves from stalkers and stalking and to allow those qualifying for using an alternative address from not standing out due to the rarity of those addresses.

The DHS Privacy Office noted, however, that Congress actually suggested that innovation might "allow for less data being present on the face of the card." PIA, at 4. All individuals should be allowed to use an alternate address at least on the card itself as a minimum "first step" in redressing the harms set to be moved into action against card holders. Alternate addresses can point to the home address in a database in a more secure location than a grocery store or other retail outlet, which is where many people's REAL IDs will be scanned.

REAL ID can burden senior citizens and others with health care issues

The NPRM also did not contemplate how senior citizens, disabled individuals, disadvantaged individuals, and others reliant on Federal health care programs such as Medicare will be impacted by REAL ID. Additionally, the NPRM makes no attempt to mitigate the profound public health harms that may result from the implementation of the Act.

SSN verification may be difficult or impossible for victims of identity theft, and in particular medical identity theft who are also recipients of Medicare. What will happen to individuals on Medicare who fail SSN verification? What is the process for recourse for people who have chronic conditions that cannot suffer a lapse of medication or service? There are known weaknesses in the SSN verification systems. Will DHS simply put this problem off on the states to handle?

Additionally, there is no procedure to ensure health care for elderly, disabled, and disadvantaged individuals on Medicare who are not able -- for a variety of reasons (cost, inability to understand, lack of mobility) to get the required identity documents. Will people be denied essential services in the name of REAL ID?

The REAL ID system is likely to facilitate discrimination

Unsurprisingly, "it appears that laws requiring individuals to show proof of legal status or citizenship result in increased discrimination based on national origin and/or appearance." IDs — NOT THAT EASY, at 7 (citing U.S. General Accounting Office, IMMIGRATION REFORM: EMPLOYER SANCTIONS AND THE QUESTION OF DISCRIMINATION, March 1990 (noting that "widespread pattern of discrimination" resulted "solely from the implementation of IRCA" (Immigration Reform and Control Act of 1986)). The NAS Committee therefore concluded that if a national ID system were deployed, "[t]he human rights issues that could arise, such as increased demands for documentation from those who look or sound 'foreign' and the deterioration of living and working conditions for aliens, are substantial." Id. at 7.

Matters may be worse with the REAL ID because the two-dimensional bar code system standard that DHS calls for in the regulation -- the PDF-417 2D bar code, which can be read by a standard 2D barcode scanner -- includes machine-readable information about race and ethnicity. DHS's chosen standard for the 2D barcode, the 2005 AAMVA

Driver's License/Identification Card Design Specifications, Annex D, includes the cardholder's race as one of the data elements.

Under this standardized format, white people would carry the designation "W"; black people would carry the designation "BK"; people of Hispanic origin would be designated "H"; Asian or Pacific Islanders would be "AP"; and Alaskan or American Indians would be "AI."

DHS does not require the "race/ethnicity" data element, but its chosen standard could be adopted in its entirety by state driver licensing bureaus. Yet DHS has done nothing to prevent or discourage the placement of race and ethnicity in the machine readable zones of this national ID card. Federal law and regulation should not promote a national ID system that can track people by race.

Security experts Forno and Schneier also note that those who do not obtain REAL IDs may be deemed suspicious. "One likely outcome of this DHS-proposed social segregation is that people presenting non-Real ID identification automatically will be presumed suspicious and perhaps subject to additional screening or surveillance to confirm their innocence at a bar, office building, airport or routine traffic stop." , http://news.com.com/2010-7348-6180835.html?tag=tb

IV. The REAL ID Act raises serious federalism concerns

The NPRM expressly asks about federalism (p. 95): "(10) The federalism aspects of the rule, particularly those arising from the background check requirements proposed herein." It also presents an analysis of federalism pursuant to Executive Order 13132 (pp. 114-122).

We believe that the Act violates both the spirit and the letter of federalism law. Our Constitution established a federal government with limited, enumerated powers in order to protect the people from undue concentration of power. "Perhaps the principal benefit of the federalist system is a check on abuses of government power.... Just as the separation and independence of the coordinate Branches of the Federal Government serve to prevent the accumulation of excessive power in any one Branch, a healthy balance of power between the States and the Federal Government will reduce the risk of tyranny and abuse from either front. . . . In the tension between federal and state power lies the promise of liberty." *Gregory v. Ashcroft,* 501 U.S. 452, 459 (1991).

A federal law that aims to conscript the states into creating a national ID system, with all the privacy and civil liberties risks discussed in Part I of these comments, is precisely the kind of scheme that the Framers expected that federalism would guard against. As of this writing, several states have passed anti-REAL ID resolutions or legislation, and similar bills have been filed in many other states. While the states are concerned about the costs of this unfunded mandate, they are also concerned about how it intrudes upon state sovereignty and civil liberties.

As one New Hampshire legislator said recently, the REAL ID Act "is probably the worst piece of blackmail to come out of the federal government. This is pure, unadulterated blackmail." Norma Love, "Representatives okay REAL ID ban," *Concord Monitor*, April 6, 2007 http://www.concordmonitor.com/apps/pbcs.dll/article?Date=200704. . . . And the governor of New Hampshire has echoed this sentiment, noting that too many

questions remained about costs and privacy and that the Act would turn state DMV workers into de facto agents of the Homeland Security Department. Id.

Federalism protects individual rights

One aspect of federalism is the protection of individual rights against government abuse. As EFF explained in Part I, the national ID system that the Act seeks to create poses enormous risks to privacy and civil liberties.

Recent federalism case law has centered around the notion of "commandeering." In exercising its power under the Commerce Clause, Congress may not "commandeer" the state regulatory processes by ordering states to enact or administer a federal regulatory program. *See, e.g., New York v United States*, 505 U.S. 144 (1992) (holding unconstitutional the "take title" provision of the 1985 Low-Level Radioactive Waste Policy Amendments Act requiring States to dispose of radioactive waste within their borders by a certain date or take on ownership and legal liability for such waste).

This anti-commandeering principle was later extended when the Supreme Court held that Congress may not circumvent the prohibition on commandeering a state's regulatory processes "by conscripting the State's officers directly." *Printz v. United States*, 521 U.S. 898, 935 (1997) (holding unconstitutional Brady Handgun Violence Prevention Act provisions that forced non-federal law enforcement officers to do background checks on gun buyers).

DHS argues that "[t]he proposed rule would not formally compel any State to issue driver's licenses or identification cards that will be acceptable for federal purposes. Importantly, under this scheme, '[a]ny burden caused by a State's refusal to regulate will fall on those [citizens who need to acquire and utilize alternative documents for federal purposes], rather than on the State as a sovereign.'" NPRM, at 120 (quoting *New York*, 505 U.S. at 173.

This defense is legal sophistry. It is equally – if not more – arguable that, because the issuance of drivers' licenses is a state regulatory function, the minimum issuance and verification requirements established in this bill, even if limited to federal agency acceptance, constitute an effective commandeering by Congress of the state regulatory process, or a conscription of the state and local officials who issue the licenses.

It is particularly disgusting that DHS would seize upon the fact that the Act's burdens fall on citizens as a defense to federalism concerns. It is obvious from the statutory structure that the States are being coerced into limiting the rights of individuals by forcing a trade between the dangers of a national ID scheme and individuals' being able to board planes, and transact with federal agencies using "valid" ID.

Finally, this defense elevates form over substance. DHS itself "recognizes that, as a practical matter, States may view noncompliance with the requirements of REAL ID as an unattractive alternative." NPRM, at 122.

Employee background checks

Federalism also seeks to protect the states as political entities against the central government. The anti-commandeering doctrine addresses the accountability problem of States being "blamed" for federal regulation, which harms to democracy to the extent that

the public is misled into venting its political ire at state officials who merely implement federal policy, rather than the federal government that created the policy. Thus, in *New York v. United States*, the statute required the state legislature to make the politically difficult decision about where to locate a facility for the disposal of radioactive waste. Congress obviously sought political credit for solving the radioactive waste problem without taking responsibility for making decisions likely to outrage voters.

This issue is especially important for the Act's background check provisions. DHS emphasized background checks as a federalism issue because in *Printz*, mentioned above, the Supreme Court held unconstitutional some provisions of the federal Brady Act, which required State and local law enforcement officers to perform background checks on handgun purchasers and related activities, because they effectively commandeered these officers to enforce federal regulations.

The Brady Act demanded that local "chief law enforcement officers" receive paperwork from gun sellers and make a "reasonable effort," within five days, to determine whether their customers fell into any of the categories forbidden by federal law to purchase guns. The Court held that it is "fundamentally incompatible with our constitutional system of dual sovereignty" for the federal government to commandeer state or local government officials to "administer or enforce a federal regulatory program." *Printz*, 521 U.S. at 935.

Importantly, *Printz* relied heavily on *Gregory*: "Just as the separation and independence of the coordinate branches of the Federal Government serve to prevent the accumulation of excessive power in any one branch, a healthy balance of power between the States and the Federal Government will reduce the risk of tyranny and abuse from either front." *Printz*, 521 U.S. at 921 (*quoting Gregory*, 501 U.S. at 458). Justice Scalia also characterized federalism as "a double security . . . to the rights of the people." Id. at 922 (quoting THE FEDERALIST NO. 51 (Alexander Hamilton)). He concluded: "The power of the Federal Government would be augmented immeasurably if it were able to impress into its service - and at no cost to itself - the police officers of the 50 States." Id.

The government argued in *Printz* that unlike in *New York*, the states were not making policy decisions and that the mere "discrete, ministerial tasks" called for by the Brady Act would not lead anyone to assign responsibility to local government rather than to Congress. Id. at 929. But Justice Scalia found that the key question was "(p)reservation of the States as independent and autonomous political entities." Id. at 928. By using the resources of local government, Congress avoided paying for the work; moreover, the local government official was stuck in the role of being the face of enforcement, the one to blame for any denial or mistake in the course of performing individual background checks, even though the sheriffs who brought the suit had publicized their opposition to the Brady Act. Id. at 929-30.

Importantly, the merits of the Brady Act were largely irrelevant to the Court's anti-commandeering analysis. The Court acknowledged that the Brady Act "serves very important purposes, is most efficiently administered by CLEOs during the interim period, and places a minimal and only temporary burden upon state officers." Id. at 931-32. Nevertheless, these arguments simply miss the point. By "resist[ing] the temptation" to approve of "an expedient solution to the crisis of the day," federalism serves the long-

term constitutional goal of individual liberty in ensuring that decentralized government could provide a "double security" for the rights of the people. Id. at 933.

Here, there is no doubt that the entire purpose of the REAL ID Act is to impress the DMVs of the 50 states into the service of the federal government. There is no doubt that the national ID system it creates endangers the privacy and civil liberties of Americans. And there is no doubt that Congress wished to avoid public scrutiny of the Act by sneaking it into a massive appropriations bill with little or no debate about its national ID system.

V. The contemplated REAL ID system lacks adequate, credible protection for privacy and other important rights

Given the dangers of any national ID system, it is unremarkable that the REAL ID Act expressly repealed statutory provisions intended to protect individuals' privacy. In this section we comment on a variety of other problems with the proposed national ID system.

Privacy is an issue of national significance

Many different federal laws and policies seek to foster privacy and data security, even in the context of national security programs. The Executive Order establishing the President's board on safeguarding Americans' civil liberties, for example, states in its very first section:

> The United States Government has a solemn obligation, and shall continue fully, to protect the legal rights of all Americans, including freedoms, civil liberties, and information privacy guaranteed by Federal law, in the effective performance of national security and homeland security functions.

E.O. 13353, Establishing the President's Board on Safeguarding Americans' Civil Liberties (Aug 27, 2004).

The Privacy Act requires federal agencies to undertake a variety of information practices, and it accords individuals a number of rights intended to protect privacy and similar interests. 5 U.S.C. §552a. The law requires agencies to extend these protections to systems of records operated "by or on behalf of the agency . . . to accomplish an agency function" when that is done by contract. 5 U.S.C. §552a(m).

While the Privacy Act apparently did not contemplate that states would maintain systems of records in furtherance of federal functions, Office of Management and Budget guidelines issued after the Privacy Act's passage say that the Act is intended to cover "de facto as well as de jure Federal agency systems." Office of Management and Budget, Privacy Act Implementation: Guidelines and Responsibilities.

The Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541 et seq. (enacted as Title III of the E-Government Act of 2002, Pub.L. 107-347), seeks to bolster information security within the federal government and for federal government functions by mandating yearly security audits. Under FISMA, the head of each agency is responsible for information security protections with regard to information systems and "information collected or maintained by or on behalf of the agency." 44 U.S.C. § 3544(a)(1)(A).

Accordingly, DHS cannot be absolved of its statutory responsibilities.

Congress expected DHS to address privacy and security issues

In the NPRM, DHS attempts to abdicate its responsibility to address privacy and security issues, saying: "The Act does not include statutory language authorizing DHS to prescribe privacy requirements for the state-controlled databases or data exchange necessary to implement the Act." NPRM, at 24 n.3.

But as the DHS Privacy Office recognized, Congress wanted DHS to address crucial privacy and security issues in the regulations.

"The House Conference Report for the REAL ID Act includes several key statements of Congressional intent regarding privacy. For example, in its discussion of section 202(d)(12) of the Act, which requires each state to provide electronic access to the information in its motor vehicle databases to all of the other states, the Conference Report makes clear that Congress recognized the need for the regulations to address privacy and security and that those protections should be at least the equivalent of existing federal protections. The Conference Report reads in relevant part:

'DHS will be expected to establish regulations which adequately protect the privacy of the holders of licenses and ID cards which meet the standards for federal identification and federal purposes.'

In addition, the Conference Report discussion of Section 202(b)(9) of the Act, which calls for using "a common machine-readable technology, with defined minimum data elements," clearly indicates that Congress wanted privacy to be a consideration in implementing the technology. The Conference Report states:

'There has been little research on methods to secure the privacy of the data contained on the machine readable strip. Improvements in the machine readable technology would allow for less data being present on the face of the card in the future, with other data stored securely and only able to be read by law enforcement officials.'"

PIA, at 4 (footnotes and italics omitted).

Thus, DHS cannot validly claim that it lacked authority to protect privacy. It simply refused to use it.

The DHS regulations do not provide for privacy or security of personal data

As discussed above, the creation of interlinked databases as well as the requirement that each DMV store copies of every birth certificate and other documents presented to it will create a one-stop shop for identity thieves, as well as other privacy problems.

The databases required by the Act are extensive. Each state's DMV database, at a minimum, will be linked and both information and documents – from SSNs and birth dates to copies of birth certificates and bank statements – will be accessible to many persons across the country. This will be a dream for identity thieves, and the potential for insider fraud and unauthorized insider issuance of false licenses is enormous.

While the DHS regulations require the states to provide information "as to how the State will protect the privacy of the data collected, used, and maintained in connection with

REAL ID, including all source documents," DHS does not require or set minimum standards for privacy protection. NPRM, at 27.

At present, there is no sign that the private sector will be prevented from using the cards for authentication or data indexing. Thus, once these cards are ubiquitous, businesses will have access to a credential that provides strong authentication, and an index number, without having to commit to any improvement in their privacy practices.

Commercial "harvesting" of REAL ID data will be facilitated by the "machine-readable technology" requirement. It is virtually certain that this technology will be available to the private sector as well as to governmental users. "And because the IDs will become standardized around one mandated technology, the cost of license-reading technology will decrease, thereby lowering the cost barrier to the collection and storage of the holders' personal data by private parties." Froomkin, 48 Boston College L. Rev. at 83.

Thus, as security expert Bruce Schneier observed, "This will, of course, make identity theft easier. Assume that this information will be collected by bars and other businesses, and that it will be resold to companies like ChoicePoint and Acxiom. It actually doesn't matter how well the states and federal government protect the data on driver's licenses, as there will be parallel commercial databases with the same information." Schneier on Security, http://www.schneier.com/blog (May 9, 2005, 09:06 EST).

DHS failed to address the issue of identity theft

The Act does not contain limitations on what personal information in a DMV database, including source documents, may be accessed, by whom, or for what purposes. The proposed regulations state: "DHS believes that it would be outside its authority to address this issue [of identity theft] within this rulemaking." NPRM, at 73.

However, 6 U.S.C. § 42 (1) states that among DHS's duties is:

> assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information.

Thus, we believe it is within DHS authority to address the issue of identity theft.

DHS failed to guide the states with respect to a comprehensive security plan

Instead, because DHS has stated that it believes it does not have the authority to address identity theft, it requires the states to devise a comprehensive security plan for safeguarding information collected, stored, or disseminated for purposes of complying with the REAL ID Act. See §37.41 (pp. 150-152); §37.55 (p. 156); §37.57 (p. 157)

A comprehensive security plan is indeed critical. Media reports about data security breaches at major institutions throughout American society have repeatedly proven to the public that the entities that collect, store, process and disseminate their personal information lack meaningful information security.

The system envisioned by the REAL ID Act contains at least four major architectural weak points: (1) access to data stored on the card itself, such as the danger of automated data harvesting by public and private entities who can, regardless of authorization, access the card's machine-readable component; (2) access to ID validation services, to the extent that DHS permits states to provide such services to other entities; (3) access to the data

channels used to transmit data required to be transmitted by the REAL ID Act; and (4) access to the backend systems themselves, including any private-sector entities that states might contract out DMV operations or data processing.

Data breach is not a trivial concern in this system. The REAL ID system will contain a complete information set ready-made for identity theft on a scale that we have not known before, and this information will be broadly disseminated to and amongst the states. DHS has suffered significant data breaches even within its own most secure environments; for example, TSA lost a hard drive containing SSNs, bank data and payroll information for about 100,000 of its employees from a controlled area at TSA headquarters. Caroline McCarthy, "TSA acknowledges potential data breach," http://news.com.com/2110-1029_3-6181890.html (May 8, 2007).

If DHS cannot protect internal employee data within its own secure, controlled environments, why should anyone trust the REAL ID system to keep secure 250 million individuals' data being shared across 56 states and other jurisdictions?

For instance, the Act provides that "other states" must have access to the state motor vehicle databases, but does not detail who in "other states" may access these databases, what information they may access and for what purposes, what they may do with the information they receive, and a host of other questions about the permissible bounds of authorized access. DHS needed to address these and similar issues.

But while DHS requires the states to devise a comprehensive security plan for safeguarding information collected, stored, or disseminated for purposes of complying with the REAL ID Act, there is virtually no guidance as to what that plan should look like.

The proposed regulations do not call for the development, implementation, and assessment of common security controls, do not provide guidance or standards for documentation of the structured process of planning adequate, cost-effective system security protection, and do not delineate responsibilities and expected behavior of all individuals who access the system.

DHS does not even produce a framework for assessing the information security and privacy impacts of the network of state motor vehicle databases and associated computer systems, including those involved in verifying documents and other data covered by the REAL ID Act. Such a framework could have defined:

--what information is collected

--why the information is being collected

--how the information will be used

--the right of individuals to decline to provide information or otherwise control information about them

--with whom the information will be shared

--how the quality and integrity of the information will be maintained

--how the system will be secured from unauthorized access and use

--how long the information will be retained

--how oversight of the system will be performed

--what privacy policies and procedures will be used to protect the information

--who will be accountable for compliance with privacy, security, and other policies

--how individuals can protect their rights in data about them.

For example, § 37.33 requires states to maintain a state motor vehicle database containing, as a minimum, the data printed on DL/ID cards, card serial numbers, SSNs, and driver's histories; it also requires states to provide all other states with electronic access to the information in the state's motor vehicle database. Yet DHS provides absolutely no privacy or security standards for this data.

Instead, § 37.41 calls for states to prepare a comprehensive security plan for DMV offices and DL/ID card storage and production facilities, including addressing safeguards to protect the security, confidentiality, and integrity of the personal information stored and maintained in DMV records and information systems. §§ 37.41, 37.55 and 37.57 require states to submit comprehensive security plans to DHS as an initial certification process and annually thereafter.

The NPRM does not define security standards or a governance structure for managing any of the shared databases and systems. This abdication places the states in an impossible position: they are being forced to make their own citizens' personal information available to every other state with no guarantee of privacy or security.

And if a state were to make a good faith effort to do so, the first thing it would realize is that it has no idea what it is to do. These databases have not been built yet. To ask the states to develop such "comprehensive security plans" without first knowing the structure of the required databases and systems makes absolutely no sense.

Moreover, if states could comply with the security requirement by developing their security plans separately, some states will have stronger security than others—but the requirement that a state must give all other states access to its database of sensitive personal information means that the state with the weakest security would make other states' systems and data vulnerable to unauthorized access, acquisition, disclosure, modification, or destruction.

A comprehensive privacy and security framework for DMV facilities and the databases mandated by the REAL ID Act is essential to the accomplishment of the Act's objective of creating more secure and reliable identity credentials. In order to ensure that a state can properly secure the personally identifiable information of its residents, it must be able to hold other states that have access to its records and systems to its security standards.

DHS deferred the critical issue of encryption

As for security of the ID itself, DHS has mentioned that encryption of the machine-readable zone (MRZ) on licenses might be preferable - but it has not mandated that states in fact encrypt the data. In fact, the NPRM specifically asks for comments on encryption of the MRZ.

We do not endorse the REAL ID, of course, but we nonetheless believe that protection of the MRZ data is necessary to prevent routine harvesting of the personal information contained therein. In California, the option of not encrypting is simply unacceptable given the importance of privacy to Californians, established by the California Constitution's guarantee of an individual's "inalienable right" to pursue and obtain "privacy" (Art. 1, sec. 1), as well as many state privacy laws. As the DHS PIA recognizes, a standardized MRZ on all states' IDs increases the likelihood of secondary uses by private sector and governmental entities, while the inclusion of the personally identifying information from the front of the card in the MRZ facilitates the creation of databases for secondary uses.

We question the need for any personal information in the MRZ, given that law enforcement officers can simply use their eyes to read the data from the face of the card. The MRZ could contain a pointer that does not correspond to any other ID number (including the REAL ID number) to a law-enforcement-access-restricted database, and that pointer could be changed each time the REAL ID is renewed.

The background check provisions are bad for privacy

DHS requires background checks of those involved in REAL ID processing. §§ 37.03 (p. 126); 37.45 (p. 153) 37.55 (p. 156); 37.57 (p. 157). Two aspects of the proposed requirement raise privacy issues. (1) The permanently disqualifying offenses are defined as conviction of the felonies listed in 49 CFR 1572.108(a). That list does not include identity theft or financial fraud, which is the most likely criminal act of a dishonest employee. (2) Requiring a financial history check as part of an employee background check would be a privacy invasion that would not provide information useful to DMV in reducing security risks.

DHS failed to address the critical privacy issues of redress, access and correction

With REAL ID, the role of the driver's license will become even more critical to the average, law-abiding citizen's ability to conduct his or her life. When problems arise, the individual will be severely hampered if resolution is not quickly and easily available.

Two of the basic privacy principles are Individual Participation, the right of individuals to access and correct their own personal information, and Accountability, including individuals' right to due process and redress when they are harmed by errors or abuses of their personal information.

An effective and timely redress process for individuals whose records contain errors, inaccuracies, or fraudulent information is essential. The ability to replicate the correction throughout the system is critical. REAL ID-based identity theft victims cannot be left in permanent legal limbo and must not be made to bear the costs of correcting their records. Timely and adequate redress would be a primary function of a federated governance structure, managed by states according to agreed upon policies.

Lack of redress will cause profound distress to individuals:

- Individuals who cannot get an SSN verified and who are on Medicare may be dropped from the rolls and may be exposed to life-threatening lapses in medical care.

- Individuals who have been victims of criminal identity theft may never be able to qualify for a REAL ID due to the actions of their imposters. These individuals may be denied healthcare, and may not be able to fly commercially or even be licensed to drive a car due to their lack of ability to defend their identity documents as accurate.
- Individuals who are recently married or divorced and who apply for a REAL ID may well fail the SSN verification, potentially disrupting their lives and ability to receive healthcare or conduct their lives in a normal manner.

DHS has put a great deal of trust in the various processes it is insisting on. But there are many intricate moving parts in the process, and DHS has not thought through the issues each part creates. For example, while SSN verification may sound like a system that is complete and accurate, SSN verification systems rely in whole or in part upon the accuracy of public records. And we also know that SSN verification can and does fail, producing both false negatives and false positives. DHS has not allowed for this in its NPRM, and this is problematic. There must be a clear, fair, plan of specific recourse and redress that is consistent. Otherwise, victims of identity theft and others will have many problems getting through the REAL ID system.

The DHS Privacy Impact Assessment did not address all of the issues raised by the REAL ID Act and NPRM.

EFF applauds the Privacy Office's attempt to conduct a privacy impact assessment, which addressed privacy issues more objectively than did the NPRM. Nevertheless, we believe the PIA failed to address some key issues.

The PIA listed four areas of inquiry or primary concern, and stated that these four areas are the "key privacy issues" posed by the Act:

> The PIA addresses the key privacy issues posed by the Act: (1) Does the REAL ID Act create a national identity card or database; (2) How will personal information required by the REAL ID Act be protected in the state databases; (3) How will the personal information stored on the machine readable technology on the driver's licenses and identification cards be protected from unauthorized collection and use; and (4) Do the requirements for a photograph and address on the credential and the DMV employee background check erode privacy. PIA, at 16.

There are, however, many substantial areas of concern that the PIA did not address, including issues relating to public safety. For example, the PIA (and the NPRM for that matter) completely ignored crucial concerns about stalking using women's real addresses contained on the card and in linked databases. The databases used by the states will be federated, and will have thousands of access points. What is to stop an individual from stalking a woman whose detailed home address information is there for the taking? And what about the dangers presented for women who will be asked by hundreds if not thousands of individuals over the course of their daily lives to see their REAL ID card? Only a subset of women meet the standard required by REAL ID for listing an alternate address; the vast majority of women will be forced to list their home address and have it be visible on their ID card. With the REAL ID plan, individuals who want to stalk a

woman will have copious opportunities based on the card and the associated nationwide databases, whereas women are left with no place to hide.

The U.S. Government Accountability Office describes what a privacy impact assessment should look like:

> . . . the E-Government Act requires agencies to describe similar privacy protections in a privacy impact assessment, which addresses what information is to be collected, the intended use of the information, with whom the information will be shared, what notices or opportunities for consent would be provided to individuals regarding what information is collected, how the information will be secured, and whether a system of records is being created. *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public,* GAO-05-864R, July 22, 2005.

Under 6 U.S.C. sec. 42 (5)(A), the law requires DHS to do the following:

> ...coordinat[e] with the Officer for Civil Rights and Civil Liberties to ensure that - (A) programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner;

Because of the information that is missing from the PIA, we do not believe that DHS has fulfilled its obligations under the E-Government Act. We also believe DHS has not fulfilled the requirements of addressing privacy considerations in a comprehensive manner under 6 U.S.C. § 42.

Conclusion

EFF and WPF appreciate the hard work of DHS and its Privacy Office in attempting to implement the ill-conceived REAL ID Act. The PIA in particular makes a serious attempt to analyze the privacy and security issues, such as with the recommendation that encryption be used to protect MRZ data. But Congress has asked for the impossible.

As a result, despite its hard work, DHS has created a plan that will cost enormous amounts of money without achieving meaningful benefits, while embedding a national ID system into everyday life. Hamstrung by the poorly drafted Act, the regulations effectively seek to enable a national ID card system without accepting or managing any of the responsibility for ensuring even the most nominal protections in the area of privacy, security, confidentiality, and identity theft.

We rarely urge an agency and Congress to completely rewind history. But there is no alternative here. DHS should suspend implementation of the REAL ID Act, and Congress should hold legislative hearings to investigate how to repair the situation. The REAL ID Act and its regulations are profoundly flawed, must not go forward in their current form, and must not go forward without robust, honest public debate and a transparent process from start to finish.

Lee Tien
Senior Staff Attorney
Electronic Frontier Foundation

Pam Dixon
Executive Director
World Privacy Forum