DEPARTMENT OF HOMELAND SECURITY
DOCKET NO. DHS 2006-0030
Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes

COMMENTS OF:

ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

AND

[EXPERTS IN PRIVACY AND TECHNOLOGY]

STEVEN AFTERGOOD
PROF. ANITA ALLEN
PROF. ANN BARTOW
PROF. JAMES BOYLE
DAVID CHAUM
SIMON DAVIES
WHITFIELD DIFFIE
PROF. DAVID FARBER
PHILIP FRIEDMAN
DEBORAH HURLEY
PROF. JERRY KANG
CHRIS LARSEN
MARY MINOW
DR. PETER G. NEUMANN
DR. DEBORAH PEEL
STEPHANIE PERRIN
PROF. ANITA RAMASASTRY
BRUCE SCHNEIER
ROBERT ELLIS SMITH
PROF. DANIEL J. SOLOVE
PROF. FRANK M. TUERKHEIMER

———

TABLE OF CONTENTS

I. INTRODUCTION

By notice published on March 9, 2007, the Department of Homeland Security ("DHS") announced it seeks to establish "minimum standards for State-issued driver's licenses and identification cards that Federal agencies would accept for official purposes after May 11, 2008, in accordance with the REAL ID Act of 2005."[1] Pursuant to this notice, the aforementioned group ("Coalition") submits these comments to request the Department of Homeland Security recommend to Congress that REAL ID is unworkable and must be repealed. The REAL ID Act creates an illegal *de facto* national identification system filled with threats to privacy, security and civil liberties that cannot be solved, no matter what the implementation plan set out by the regulations.[2] And if REAL ID implementation does go forward, the protections of the Privacy Act of 1974 must be fully enforced for all uses of the data current and feature. Agencies should not be permitted to assert any exemptions and individuals must granted all rights, including the judicially enforceable right to access and correct their records and to ensure compliance with all of the requirements of the Privacy Act.

The problematic adoption of the law now under consideration is now well known. The REAL ID Act was appended to a bill providing tsunami relief and military appropriations, and passed with little debate and no hearings. It was passed in this manner

---

[1] Dep't of Homeland Sec., *Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, 72 Fed. Reg. 10,819 (Mar. 9, 2007) ["REAL ID Draft Regulations"], *available at* http://a257.g.akamaitech.net/7/257/2422/01jan20071800/edocket.access.gpo.gov/2007/07-1009.htm; *see generally*, EPIC, *National ID Cards and the REAL ID Act Page*, http://www.epic.org/privacy/id_cards/; EPIC, Spotlight on Surveillance, *Federal REAL ID Proposal Threatens Privacy and Security* (Mar. 2007), http://www.epic.org/privacy/surveillance/spotlight/0307; Anita Ramasastry, *Why the New Department of Homeland Security REAL ID Act Regulations are Unrealistic: Risks of Privacy and Security Violations and Identity Theft Remain, and Burdens on the States Are Too Severe*, Findlaw, Apr. 6, 2007, *available at* http://writ.news.findlaw.com/ramasastry/20070406.html.

[2] Pub. L. No. 109-13, 119 Stat. 231 (2005).

even though Republican and Democratic lawmakers in the Senate urged Senate Majority Leader Bill Frist to allow hearings on the bill and to permit a separate vote on the measure.[3] The senators said they believe REAL ID "places an unrealistic and unfunded burden on state governments and erodes Americans' civil liberties and privacy rights."[4] The people could not speak during this rushed process. They are speaking now.

II. REAL ID CREATES A NATIONAL ID SYSTEM

Throughout the history of the United States, its people have rejected the idea of a national identification system as abhorrent to freedom and democracy. The REAL ID Act and the draft regulations to implement it create a *de facto* national identification system, and the Act must be repealed.

A. Americans Have Consistently Rejected a National ID System

When the Social Security Number (SSN) was created in 1936, it was meant to be used only as an account number associated with the administration of the Social Security system.[5] Though use of the SSN has expanded considerably, it is not a universal identifier and efforts to make it one have been consistently rejected.[6] In 1973, the Health, Education and Welfare Secretary's Advisory Committee on Automated Personal Data Systems rejected the creation of a national identifier and advocated the establishment of significant safeguards to protect personal information. The committee said:

---

[3] Press Release, S. Comm. on Homeland Sec. & Governmental Affairs, Twelve Senators Urge Frist To Keep Real ID Act Off Supplemental Appropriations Bill Sweeping Proposal Needs Deliberate Consideration (Apr. 12, 2005), *available at* http://www.senate.gov/%7Egov_affairs/index.cfm?FuseAction=PressReleases.Detail&Affiliation=R&PressRelease_id=953&Month=4&Year=2005.

[4] *Id.*

[5] EPIC & PRIVACY INT'L, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND PRACTICE 47 (EPIC 2004).

[6] *See* Marc Rotenberg, Exec. Dir., EPIC, *Testimony and Statement for the Record at a Hearing on Social Security Number High Risk Issues Before the Subcomm. on Social Sec., H. Comm on Ways & Means*, 109th Cong. (Mar. 16, 2006), *available at* http://www.epic.org/privacy/ssn/mar_16test.pdf; EPIC page on Social Security Numbers, http://www.epic.org/privacy/ssn/.

> We recommend against the adoption of any nationwide, standard, personal identification format, with or without the SSN, that would enhance the likelihood of arbitrary or uncontrolled linkage of records about people, particularly between government or government-supported automated personal data systems. What is needed is a halt to the drift toward [a standard universal identifier] and prompt action to establish safeguards providing legal sanctions against abuses of automated personal data systems.[7]

In 1977, the Carter Administration reiterated that the SSN was not to become an identifier. In Congressional testimony in 1981, Attorney General William French Smith stated that the Reagan Administration was "explicitly opposed to the creation of a national identity card."[8] When it created the Department of Homeland Security, Congress made clear in the enabling legislation that the agency could not create a national ID system.[9] In September 2004, then-Department of Homeland Security Secretary Tom Ridge reiterated, "[t]he legislation that created the Department of Homeland Security was very specific on the question of a national ID card. They said there will be no national ID card."[10] The citizens of the United States have consistently rejected the idea of a national identification system.

B. REAL ID Is Not Voluntary

Supporters of REAL ID point to the legislation, which says that State implementation is "voluntary." However, States are under considerable pressure to implement REAL ID and citizens who fail to carry the new identity document will find it impossible to pursue many routine activities, The administration has also pursued a

---

[7] Dep't of Health, Educ. & Welfare, Sec'y's Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* (July 1973), *available at* http://www.epic.org/privacy/hew1973report/.
[8] Robert B. Cullen, *Administration Announcing Plan*, Associated Press, July 30, 1981.
[9] Pub. L. No. 107-296, 116 Stat. 2135 (2002).
[10] Tom Ridge, Sec'y, Dep't of Homeland Sec., *Address at the Center for Transatlantic Relations at Johns Hopkins University: "Transatlantic Homeland Security Conference"* (Sept. 13, 2004), *available at* http://www.dhs.gov/xnews/speeches/speech_0206.shtm.

heavy-handed assault on those who have raised legitimate questions about the efficacy, cost, and impact of the $23B program. Critics of REAL ID have been labeled anti-security. In Congressional testimony, a high-ranking DHS official said, "Any State or territory that does not comply increases the risk for the rest of the Nation."[11] It is not anti-security to reject a national identification system that does not add to our security protections, but in fact makes us weaker as a nation. This system is also an unfunded mandate that imposes an enormous burden upon the states and the citizenry. The federal government has estimated that REAL ID will cost $23.1 billion, but it has allocated only $40 million for implementation and has told the states that they may divert homeland security grant funding already allocated to other security programs for REAL ID.[12]

Design standardization means that anyone with a different license or ID card would be instantly recognized, and immediately suspected. The Department of Homeland Security already contemplates expanding the REAL ID card into "everyday transactions."[13] It will be easy for insurance firms, credit card companies, even video stores, to demand a REAL ID driver's license or ID card in order to receive services. Significant delay, complication and possibly harassment or discrimination would fall upon those without a REAL ID card. In actuality, the "voluntary" card is the centerpiece of a *mandatory* national identification system that the federal government seeks to impose on the states and the citizens of the United States.

---

[11] Richard C. Barth, Ass't Sec'y for Policy Development, Dep't of Homeland Sec., *Testimony at a Hearing on Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers' Licenses and Identification Cards Before the Subcomm. on Oversight of Gov't Management, the Federal Workforce & the District of Columbia, S. Comm. on Homeland Sec. & Governmental Affairs*, 110th Cong. (Mar. 26, 2007) ["DHS Testimony at REAL ID Hearing"], *available at* http://hsgac.senate.gov/_files/Testimonybarth.pdf.

[12] REAL ID Draft Regulations at 10,845, *supra* note 1.

[13] *See* Data Collection Expansion discussion, *infra* Section IX (DHS plans to expand uses of REAL ID).

C. Regulations Create a De Facto National ID System

The Department of Homeland Security draft regulations would (1) impose more difficult standards for acceptable identification documents that could limit the ability of individuals to get a state drivers license; (2) compel data verification procedures that the Federal government itself is not capable of following; (3) mandate minimum data elements required on the face of and in the machine readable zone of the card; (4) require changes to the design of licenses and identification cards (5) expand schedules and procedures for retention and distribution of identification documents and other personal data; and (6) dictate security standards for the card, state motor vehicle facilities, and the personal data and documents collected in state motor vehicle databases. These regulations create a *de facto* national identification system.

State licenses and identification cards must meet standards set out in the regulations to be accepted for Federal use. REAL ID cards will be necessary for: "accessing Federal facilities, boarding commercial aircraft, and entering nuclear power plants."[14] The Supreme Court has long recognized that citizens enjoy a constitutional right to travel. In *Saenz v. Roe*, the Court noted that the "'constitutional right to travel from one State to another' is firmly embedded in our jurisprudence."[15] For that reason, any government initiative that conditions the ability to travel upon the surrender of privacy rights requires particular scrutiny. This is particularly relevant under the REAL ID regulations, as they affect 245 million license and cardholders nationwide. REAL ID could preclude citizens from entering Federal courthouses to exercise their right to due

[14] REAL ID Draft Regulations at 10,823, *supra* note 1.
[15] 526 U.S. 489 (1999), quoting *United States v. Guest*, 383 U.S. 745 (1966).

process, or from entering Federal agency buildings in order to receive their Social Security or veterans' benefits.

DHS may compel card design standardization, "whether a uniform design/color should be implemented nationwide for non-REAL ID driver's licenses and identification cards," so that non-REAL ID cards will be easy to spot.[16] This universal card design will lead to a national identification system, combined with the mandate under the proposed regulations imposing new requirements on state motor vehicle agencies so that the Federal government can link together their databases to distribute license and cardholders' personal data, create a national identification system.[17] DHS also has considered expanding the official uses for the REAL ID system, going so far as to estimate that one of the ancillary benefits of REAL ID implementation would be to reduce identity theft – a reduction DHS bases on "the extent that the rulemaking leads to incidental and required use of REAL ID documents in everyday transactions."[18] There are other ways in which DHS has contemplated expanding the uses of the REAL ID system so that the card becomes a national identifier – one card for each person throughout the country.[19]

III. DHS HAS THE OBLIGATION TO PROTECT PRIVACY OF CITIZENS

The Department of Homeland Security states that it is constrained in its power to protect the privacy of individuals and their data under the REAL ID Act. The agency claims in the notice of proposed regulations that "The Act does not include statutory

[16] REAL ID Draft Regulations at 10,841, *supra* note 1.
[17] *Id.* at 10,825.
[18] Dep't of Homeland Sec., *Regulatory Evaluation; Notice of Proposed Rulemaking; REAL ID; 6 CFR Part 37; RIN: 1061-AA37; Docket No. DHS-2006-0030*, at 130 (Feb. 28, 2007) ["Regulatory Evaluation"], *available at* http://www.epic.org/privacy/id_cards/reg_eval_draftregs.pdf.
[19] *See* Data Collection Expansion discussion, *infra* Section IX (DHS plans to expand uses of REAL ID).

language authorizing DHS to prescribe privacy requirements for the state-controlled databases or data exchange necessary to implement the Act."[20] We agree with Sen. Joseph Lieberman, who stated, "The concept that federal agencies need explicit Congressional authorization to protect Americans' privacy is just plain wrong. In fact, our government is obligated to ensure that programs and regulations do not unduly jeopardize an individual's right to privacy."[21]

The draft regulations include little in terms of privacy safeguards:

> In summary, DHS has proposed the following privacy protections in its implementing regulations for the REAL ID Act: (1) The State-to-State data exchanges and the State data query of Federal reference databases will be State operated and governed; (2) as part of the State certification process, States will be required to submit a comprehensive security plan, including information as to how the State implements fair information principles; and (3) while acknowledging the benefits of employing encryption of the personal information stored on the identification cards, we invite comment on its feasibility and costs and benefits to ensure that its costs do not outweigh the benefits to privacy.[22]

DHS's statement that it is constrained in its ability to set privacy protections for the REAL ID system is a product of the agency's mistaken belief that security and privacy are separate. Security and privacy are intertwined; one cannot have a secure system if privacy safeguards are not created, as well. DHS stated that it "believes that this language [in the REAL ID Act] provides authority for it to define basic security program requirements to ensure the integrity of the licenses and identification cards."[23] Because DHS has the authority to define basic security requirements, it also has the authority to set basic privacy safeguards for the REAL ID system.

---

[20] REAL ID Draft Regulations at 10,825, *supra* note 1.
[21] Joseph Lieberman, U.S. Senator, *Statement at a Hearing on Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers' Licenses and Identification Cards Before the Subcomm. on Oversight of Gov't Management, the Federal Workforce & the District of Columbia, S. Comm. on Homeland Sec. & Governmental Affairs*, 110th Cong. (Mar. 26, 2007).
[22] REAL ID Draft Regulations at 10,826, *supra* note 1.
[23] *Id.*

The draft regulations create a national identification system that affects 245 million license and cardholders nationwide, yet DHS is hesitant to ensure strong privacy safeguards in the system itself. DHS has the obligation to protect the privacy of citizens affected by this system and must do more than the feeble attempts set out in the draft regulations.

A. Privacy Act Applies Under OMB Guidelines

The Department of Homeland Security states that the Privacy Act of 1974[24] applies to only one part of the REAL ID system – the Problem Driver Pointer System.[25] However, the Privacy Act of 1974 applies to the entire national identification system, under guidelines set out by the Office of Management and Budget ("OMB") and the Department of Homeland Security itself.

The OMB guidelines explain that the Privacy Act "stipulates that systems of records operated under contract or, in some instances, State or local governments operating under Federal mandate 'by or on behalf of the agency . . . to accomplish an agency function' are subject to . . . the Act."[26] The guidelines also explain that the Privacy Act "make[s] it clear that the systems 'maintained' by an agency are not limited to those operated by agency personnel on agency premises but include certain systems operated pursuant to the terms of a contract to which the agency is a party."[27] The REAL ID system is operated under a Federal mandate to accomplish several agency functions, including immigration control.

---

[24] 5 U.S.C. § 552a.
[25] REAL ID Draft Regulations at 10,826, *supra* note 1.
[26] Office of Mgmt. & Budget, *Privacy Act Implementation: Guidelines and Responsibilities*, 40 Fed. Reg. 28,948, 28,951 (July 9, 1975) ["OMB Guidelines"], *available at* http://www.whitehouse.gov/omb/inforeg/implementation_guidelines.pdf.
[27] *Id.*

The REAL ID system is covered by the Privacy Act under the Department of Homeland Security's own policies. In a policy guidance memorandum from the agency's Privacy Office, defines "DHS Information Systems" as "an Information System operated, controlled, or directed by the U.S. Department of Homeland Security. This definition shall include information systems that other entities, including private sector organizations, operate on behalf of or for the benefit of the Department of Homeland Security."[28] The national system of interconnected State databases is "operate[d] on behalf of or for the benefit" of DHS. The Privacy Office also states:

> As a matter of DHS policy, any personally identifiable information (PII) that is collected, used, maintained, and/or disseminated in connection with a mixed system by DHS shall be treated as a System of Records subject to the Privacy Act regardless of whether the information pertains to a U.S. citizen, Legal Permanent Resident, visitor, or alien.[29]

It is clear that, under both DHS and OMG guidelines, the REAL ID national identification system is a system of records subject to the requirements and protections of the Privacy Act of 1974.

B. Requirements of Notice, Access, Correction and Judicially Enforceable Redress Must Be Mandated

If the Department of Homeland Security creates this system, the agency must fully apply Privacy Act requirements of notice, access, correction, and judicially enforceable redress to the entire REAL ID national identification system. Though the States are asked to include provisions for notice, access, correction and redress, this is not enough. The Privacy Act protections must be mandated in the REAL ID implementation regulations.

---

[28] Privacy Office, Dep't of Homeland Sec., *Privacy Policy Guidance Memorandum* 2 (Jan. 19, 2007), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.
[29] *Id.* at 1.

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal data that Federal agencies could collect and required agencies to be transparent in their information practices.[30] In 2004, the Supreme Court underscored the importance of the Privacy Act's restrictions upon agency use of personal data to protect privacy interests, noting that:

> "[I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies." Privacy Act of 1974, §2(a)(5), 88 Stat. 1896. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements.[31]

The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]"[32] It is also intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[33] It thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[34]

We support the Department of Homeland Security's requirement that the States must include in their "comprehensive security plan" an outline of "how the State will

---

[30] S. Rep. No. 93-1183 at 1 (1974).
[31] *Doe v. Chao*, 540 U.S. 614, 618 (2004).
[32] S. Rep. No. 93-1183 at 1.
[33] Pub. L. No. 93-579 (1974).
[34] *Id.*

protect the privacy of personal information collected, disseminated or stored in connection with the issuance of REAL ID licenses from unauthorized access, misuse, fraud, and identity theft" and that the State has followed the Fair Information Practices (these are practices, not principles, as listed in the draft regulations), which "call for openness, individual participation (access, correction, and redress), purpose specification, data minimization, use and disclosure limitation, data quality and integrity, security safeguards, and accountability and auditing."[35] However, this is not enough. The agency must mandate minimum security and privacy safeguards, which the states should build upon, to protect individuals and their personal information. Also, there must be standards for the issue of redress. How will redress be adjudicated if one State includes erroneous information in an individual's file and passes that information on to another State? Will the individual have to petition both States separately for redress? Will neither State process the redress, because each believes it to be the responsibility of the other? The right of redress must be judicially enforceable.

The right of redress is internationally recognized. The Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data recognize that "the right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard."[36] The rights of access and correction are central to what Congress sought to achieve through the Privacy Act:

---

[35] REAL ID Draft Regulations at 10,826, *supra* note 1.

[36] The OECD Privacy Guidelines of 1980 apply to "personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties." Org. for Econ. Co-operation & Dev., *Guidelines Governing the Protection of Privacy and Trans-Border Flow of Personal Data, OECD Doc. 58 final* at Art. 3(a) (Sept. 23, 1980), *reprinted in* M. ROTENBERG ED., THE PRIVACY LAW

> The committee believes that this provision is essential to achieve an important objective of the legislation: Ensuring that individuals know what Federal records are maintained about them and have the opportunity to correct those records. The provision should also encourage fulfillment of another important objective: maintaining government records about individuals with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to individuals in making determinations about them.[37]

The Privacy Act requirements that an individual be permitted access to personal information, that an individual be permitted to correct and amend personal information, and that an agency assure the reliability of personal information for its intended use must be applied to the entire REAL ID national identification system. Full application of the Privacy Act requirements to government record systems is the only way to ensure that data is accurate and complete, which is especially important in this context, where mistakes and misidentifications are costly.

IV. REAL ID CARDS MUST NOT DENOTE CITIZENSHIP STATUS

DHS is considering using the REAL ID card in the Western Hemisphere Travel Initiative border security program. For the REAL ID card to be compliant under the program, it would need to include long-range RFID technology, discussed below, and "the State would have to ensure that the State-issued REAL ID driver's license or identification card denoted citizenship."[38] It cannot be stressed strongly enough: **REAL ID cards must not include citizenship status.** If REAL ID cards were to signify citizenship, there would be intense scrutiny of and discrimination against individuals who chose not to carry the national identification card and those who "look foreign."

SOURCEBOOK 2004 395 (EPIC 2005. The OECD Privacy Guidelines require, among other things, that there should be limitations on the collection of information; collection should be relevant to the purpose for which it is collected; there should be a policy of openness about the information's existence, nature, collection, maintenance and use; and individuals should have rights to access, amend, complete, or erase information as appropriate. *Id*.

[37] H.R. Rep. No. 93-1416 at 15 (1974).

[38] REAL ID Draft Regulations at 10,842, *supra* note 1.

V. STANDARDS FOR ID DOCUMENTS WOULD BURDEN MANY INDIVIDUALS

Under the REAL ID Act, States are required to obtain and verify documents from applicants that establish "(1) The applicant's identity, through a photo identity document, or a non-photo identity document that includes full legal name and date of birth if a photo identity document is not available; (2) Date of birth; (3) Proof of SSN or ineligibility for an SSN; (4) The applicant's address of principal residence; and (5) Lawful status in the United States."[39] Under the regulations, the only documents that could be accepted by the states to issue these new identity cards would be: (1) valid unexpired U.S. passport or the proposed passport card under the Western Hemisphere Travel Initiative; (2) certified copy of a birth certificate; (3) consular report of birth abroad; unexpired permanent resident card; unexpired employment authorization document; (4) unexpired foreign passport with valid U.S. visa affixed; (5) U.S. certificate of citizenship; U.S. certificate of naturalization; or (6) REAL ID driver's license or identification card (issued in compliance with the final regulations).[40]

The difficult standards for acceptable identification documents would limit the ability of some individuals to get a state driver's license. There are questions as to whether some citizens could produce these documents, among them Native Americans, victims of natural disasters, domestic violence victims, the homeless, military personnel, or elderly individuals.[41] We applaud the Department of Homeland Security for attempting to resolve this problem by allowing the States to voluntarily create an exceptions process for extraordinary circumstances. However, though DHS set minimum standards for data

[39] *Id*. at 10,827.
[40] *Id*. at 10,827-28.
[41] *See* Domestic Violence discussion, *infra* Section XI (how domestic violence victims will be harmed by the standards); *see* Data Verification discussion, *infra* Section VI (general problems with the standards).

collection, retention and documentation of the transaction, the agency did not set minimum standards for eligibility, length of process, or cost of process.[42] DHS states that persons born before 1935 might not have been issued birth certificates, so they might be eligible for the exceptions process.[43] Otherwise, there is nothing that explains to either States or individuals how they could prove eligibility, how long the process would take (days, weeks, months or even years), or if they could even afford the cost of the exceptions process.

VI. DATA VERIFICATION PROCEDURES ARE BASED ON FAULTY PREMISES

The data verification procedures mandated by the draft regulations are based on faulty premises: DHS relies on non-existing, unavailable or incomplete databases and the mistaken belief that DMV workers can or should be turned into Federal immigration officers. Each assumption creates more problems in the Department of Homeland Security's attempt to create a fundamentally flawed national identification system.

A. DHS Relies on Verification Databases That Are Not Available

Under REAL ID, the states must verify applicant documents and data with the issuing agency. DHS states that, "[f]or individual States to verify information and documentation provided by applicants, each State must have electronic access to multiple databases and systems . . . . Secure and timely access to trusted data sources is a prerequisite for effective verification of applicant data."[44] Yet, beyond the national identification system created by the State-to-State data exchange, two of four verification systems required are not available on a nationwide basis and third does not even exist.

[42] REAL ID Draft Regulations at 10,834, *supra* note 1.
[43] *Id*. at 10,822.
[44] *Id*. at 10,833.

The database systems the States are required to verify applicant information against are: (1) Electronic Verification of Vital Events ("EVVE"), for birth certificate verification; (2) Social Security On-Line Verification ("SSOLV"), for Social Security Number verification; (3) Systematic Alien Verification for Entitlements ("SAVE"), for immigrant status verification; and (4) a Department of State system to verify data from "U.S. Passports, Consular Reports of Birth, and Certifications of Report of Birth."[45]

The only system that is available for nationwide deployment is SSOLV, and a survey of States by the National Governors Association found that even this database would need substantial improvements to be able to handle the workload that would be needed under REAL ID.[46] EVVE is currently in pilot phase and only five states are participating.[47] Yet DHS bases its requirements on the assumption that EVVE will be ready for nationwide expansion by the implementation deadline May 2008.[48] The executive director of the organization overseeing the database has announced that EVVE will not be ready by May 2008 and the system may not be ready by the extended implementation deadline of December 2009.[49]

DHS admits that only 20 states are using SAVE, and that the planned connection between SAVE and another database for foreign student status verification (Student and Exchange Visitor Information System, "SEVIS") may not be completed by the

[45] *Id*. at 10,830-35; Electronic Verification of Vital Events ("EVVE") is also called Electronic Verification of Vital Event Records ("EVVER") in some federal documents.
[46] Nat'l Governors Ass'n, et. al, *The REAL ID Act: National Impact Analysis* (Sept. 19, 2006) ["Governors' Analysis"], *available at* http://www.nga.org/Files/pdf/0609REALID.PDF.
[47] Nat'l Ass'n for Public Health Statistics & Info. Systems, *Electronic Verification of Vital Events (EVVE)*, http://www.naphsis.org/projects/index.asp?bid=403.
[48] REAL ID Draft Regulations at 10,831, *supra* note 1.
[49] Eleanor Stables, *Multi-Billion Dollar Real ID Program May Be Stymied Due to $3 Million Shortfall*, CQ, Mar. 15, 2007.

implementation deadline of May 2008.[50] The State Department system to verify passports and some reports of births has not even been created, but DHS bases its mandates on the assumption that the system "is eventually developed."[51]

B. DMV Workers Cannot and Should Not Become Immigration Officials

Under the regulations, State DMV employees would need to authenticate license and identification card applicants' source documents, which means the employees would be required to physically inspect the documents and "verify[] that the source document presented under these regulations is genuine and has not been altered."[52] These source documents are: (1) valid unexpired U.S. passport or the proposed passport card under the Western Hemisphere Travel Initiative; (2) certified copy of a birth certificate; (3) consular report of birth abroad; unexpired permanent resident card; unexpired employment authorization document; (4) unexpired foreign passport with valid U.S. visa affixed; (5) U.S. certificate of citizenship; U.S. certificate of naturalization; or (6) REAL ID driver's license or identification card (issued in compliance with the final regulations).[53]

State DMV employees would be required to verify these documents, including Federal immigration documents, though they have no training to do so. DHS contemplates this problem and seeks to solve it by requiring that DMV employees handling source documents undergo 12 hours of "fraudulent document recognition" training.[54] A review of the Social Security Administration found that staff had difficulty recognizing counterfeit documents, though it is their primary job to verify these

[50] REAL ID Draft Regulations at 10,833, *supra* note 1.
[51] *Id*. at 10,832.
[52] *Id*. at 10,850.
[53] *Id*. at 10,827-28.
[54] Regulatory Evaluation at 122, *supra* note 18.

documents before issuing SSN. For example, the Government Accountability Office review reported difficulty with detection of fraudulent birth certificates. In one case, a fake in-state birth certificate was detected, but "SSA staff acknowledged that if a counterfeit out-of-state birth certificate had been used, SSA would likely have issued the SSN because of staff unfamiliarity with the specific features of numerous state birth certificates."[55] It is questionable how well State DMV employees would be able to spot fraudulent documents, especially documents as rarely seen as consular reports of birth abroad, with merely 12 hours of training when it is difficult for counterfeit documents to be spotted by federal employees whose primary job is verification of source documents. Also, if a State DMV employee determines that an applicant's source documents are fraudulent, where could the applicant turn? No redress procedure has been created.[56]

VII. MINIMUM DATA ELEMENTS ON MRT MUST REMAIN MINIMUM

Under REAL ID, the following amount of information, at a minimum, must be on the REAL ID card: (1) full legal name; (2) date of birth; (3) gender; (4) driver's license or identification card number; (5) digital photograph of the person; (6) address of principal residence; (7) signature; (8) physical security features; (9) a common machine readable technology, with defined minimum data elements; and, (10) card issue and expiration date.[57] The REAL ID card will include a 2D barcode as its machine readable technology. To protect privacy and improve security, this machine readable technology must either include encryption, which is recommended by the DHS Privacy Office, or access must be limited in some other form. Leaving the machine readable zone open would allow

[55] Gov't Accountability Office, *Social Security Administration: Actions Taken to Strengthen Procedures for Issuing Social Security Numbers to Noncitizens, but Some Weaknesses Remain*, GAO-04-12 (Oct. 2003), *available at* http://www.gao.gov/cgi-bin/getrpt?GAO-04-12.
[56] *See* Privacy Act discussion, *supra* Section III.
[57] REAL ID Draft Regulations at 10,8435, *supra* note 1.

unfettered third-party access to the data and leave 245 million license and cardholders nationwide at risk for individual tracking.

A. Access to Data Must Be Limited

Under the required changes to the design of State licenses and identification cards, DHS states the card must include "[p]hysical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purpose" and "common [machine-readable technology], with defined minimum data elements."[58] The Federal agency will require the use of a two-dimensional bar code, but will not require the use of encryption. Though Homeland Security lays out the privacy and security problems associated with creating an unencrypted machine readable zone on the license, it does not require encryption because there are concerns about "operational complexity."[59]

The Department of Homeland Security's own Privacy Office has urged the use of encryption in REAL ID cards. In its Privacy Impact Assessment of the draft regulations, the Privacy Office supported encryption "because 2D bar code readers are extremely common, the data could be captured from the driver's licenses and identification cards and accessed by unauthorized third parties by simply reading the 2D bar code on the credential" if the data is left unencrypted.[60] DHS says that, "while cognizant of this problem, DHS believes that it would be outside its authority to address this issue within

[58] *Id*. at 10,835.
[59] *Id*. at 10,826.
[60] Dep't of Homeland Sec. Privacy Office, *Privacy Impact Assessment for the REAL ID Act* 16 (Mar. 1, 2007) ["Privacy Impact Assessment of Draft Regulations"], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realid.pdf *and* http://www.epic.org/privacy/id_cards/pia_030107.pdf.

this rulemaking."[61] As we have previously stated, DHS has the obligation to protect the privacy of individuals from whom they collect data, and the agency should not abdicate this responsibility.[62] Imposing a requirement for the States to use unencrypted machine readable technology renders the cardholder unable to control who receives her data.

If, however, the agency determines that it will not use encryption because of concerns about the complexity of public key regulation, there is another approach that would better protect the privacy of individuals than unfettered access to the machine readable zone. We suggest that no personal data be placed on the machine readable zone. Instead, place a new identifier that is unused elsewhere (*i.e.*, not the driver's license number or Social Security Number). This unique identifier will "point" to the records in the national database. Access to the database can be controlled by password and encryption security, because it is easier to regulate public keys in this scenario. Also, the State should ensure that a new unique identifier is created each time the machine readable zone is renewed or reissued, in order to make the identifier less useful as an everyday ID number – people would not be forever linked to this identifier. This approach would improve data security and privacy.

It is possible to use a "pointer" system in the machine readable zone, because the REAL ID Act did not set out what minimum document requirements on the machine readable zone need to be. The Act reads, "(9) a common machine-readable technology, with defined minimum data elements."[63] Also, in the draft regulations, DHS requests comments on "[w]hether the data elements currently proposed for inclusion in the

[61] REAL ID Draft Regulations at 10,837, *supra* note 1.
[62] *See* Privacy Act discussion, *supra* Section III (federal agencies have the obligation to protect the privacy rights of individuals from whom they collect information).
[63] Pub. L. No. 109-13, 119 Stat. 231, 312, § 202(b)(9) (2005).

machine readable zone of the driver's license or identification card should be reduced or expanded."[64] We recommend against putting any personal data on the machine readable zone and only placing this unique identifier. In this way, access to the data can be more tightly controlled.

DHS is required to include security protections on the REAL ID card. Under the REAL ID Act, the card must include "(8) Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for any fraudulent purpose."[65] If DHS does not seek to limit access to the data on the REAL ID card, then it is signaling that it is acceptable for third parties to download, access and store the data for purposes beyond the three official purposes set out in the draft regulations: "accessing Federal facilities, boarding commercial aircraft, and entering nuclear power plants."[66] Though DHS has contemplated expanding the uses for the REAL ID card, such an expansion would harm both individual privacy and security and quickly turn the United States into a country where the national identification card is involuntarily carried by everyone.

B. Unfettered Data Access Threatens Individual Privacy

If personal data is placed on the machine readable zone of the REAL ID card, then access to this data must be limited or individual privacy will be threatened. Unlimited access to this data will allow unauthorized third parties to download, access and store the personal data of any REAL ID cardholder.

The REAL ID Act mandates that the REAL ID card include "(8) Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for

[64] REAL ID Draft Regulations at 10,842, *supra* note 1.
[65] Pub. L. No. 109-13, 119 Stat. 231, 312, § 202(b)(8) (2005).
[66] REAL ID Draft Regulations at 10,823, *supra* note 1.

any fraudulent purpose."[67] Allowing universal access to personal data contained on the REAL ID card would facilitate identity theft and security breaches. In the privacy impact assessment of the draft regulations, the Department of Homeland Security Privacy Office urges encryption for the REAL ID machine readable zone. It explains that unsecured digital data raises the risk of "skimming," where one "expos[es] the information stored on the credential to unauthorized collection."[68] This risk is not theoretical, the Privacy Office says, because "[r]eaders for the 2D bar code are readily available for purchase on the Internet and at a very low cost, which permits unauthorized third parties to skim the information for their own business needs or to sell to other third parties."[69] Such skimming is often done without the individual's knowledge or consent.

A recent case illustrates the security threat posed by open access to personal data on a machine readable technology. Last month, New York prosecutors charged thirteen people in a counterfeiting ring where restaurant servers on the East Coast (from Connecticut to Florida) skimmed data from customers' credit cards.[70] "They used small hand-held devices, about the size of a cigarette package that could be kept in a pocket, to record information encoded in the magnetic strips of credit cards."[71] For a year and a half, the illegally gathered data was used to create fake credit cards and buy merchandise that the criminals resold.[72] The financial data was easily accessed, downloaded and misused by the criminals because anyone with a skimmer device was able to read the unprotected machine readable zones.

---

[67] Pub. L. No. 109-13, 119 Stat. 231, 312, § 202(b)(8) (2005).
[68] Privacy Impact Assessment of Draft Regulations at 14.
[69] Privacy Impact Assessment of Draft Regulations at 14.
[70] Anemona Hartocollis, *$3 Million Lost to Fraud Ring, Authorities Say*, N.Y. Times, April 21, 2007.
[71] *Id.*
[72] *Id.*

Some States are already facing problems with unauthorized parties accessing license and ID card data. California, Nebraska, New Hampshire, and Texas have laws restricting the skimming of such data.[73] In November, the New Jersey Motor Vehicle Commission sent letters to bar, restaurant and retail organizations explaining that they must stop scanning and downloading their patrons' license data.[74] Such actions violate the state Digital Driver License Act, as well as the state and federal Drivers Privacy Protection Acts, according to the commission.[75] Yet at least one establishment expressed reluctance to stop downloading and storing their customers' personal data, even in the face of legal action from the State.[76] Today, different States have different ID cards with a variety of data and security features. Imagine what would happen if 245 million cards nationwide had personal data in the exact same open access format.

When a person hands over her license or ID card today, the data is not routinely downloaded and stored. A grocery store clerk or club bouncer usually merely looks at the card, verifies age or address, and then hands the card back to the individual. No transaction is recorded. However, universal access to the machine readable zone of the REAL ID card would allow the data to be downloaded, stored and transferred without the knowledge or permission of the individual cardholder. A digital transaction would be recorded and a digital trail could be created.

For example, let's follow Douglas Osborne for one weekend in the near future, if the national identification system is created and the machine readable zone left open for universal access. On Friday night, Doug went to Eighteenth Street Lounge at 8 p.m. with

[73] Privacy Impact Assessment of Draft Regulations at 15.
[74] Ian T. Shearn, *License scanning is illegal, state says*, Star-Ledger (NJ), Nov. 23, 2006.
[75] *Id.*
[76] *Id.*

four friends, where their REAL ID cards were scanned and their personal data accessed and stored. At 9:35 p.m., he went to Club Five with the same four friends, where their REAL ID cards were scanned and their personal data accessed and stored. On Saturday afternoon, Doug bought two six-packs of Harpoon beer at 12:27 p.m. at a Safeway in Capitol Hill, where Doug's REAL ID data was scanned and stored. On Saturday night, Doug and two friends took the 5:10 flight to Atlantic, where their cards were scanned and their information stored.[77] At 11:37 p.m., Doug and his two friends checked into a hotel, where their ID cards were scanned and their data downloaded. On Sunday morning, one of Doug's friends buys cigarettes at a casino, and his REAL ID is scanned and his data stored at 11:04 a.m. The digital trail could continue indefinitely. Individuals could easily be tracked from location to location as they went about their daily lives. Add to the REAL ID trail the information that could be gleaned from individuals' credit card transactions, and you have complete consumer profiles for which many companies would pay dearly.

DHS must include in restrictions against the addition of data beyond that defined in the REAL ID Act. To allow additional data on the machine readable zone is to increase the likelihood of the REAL ID card becoming the default identification documents for everyday transactions; this would increase the incentive for third parties to gather and store individuals' data, and substantially increase the card's value to marketers and criminals. Expansion of the data collected, uses allowed, and users authorized would greatly increase both threats to the security and privacy of personal data.

[77] "Because REAL IDs use a common MRT, the Transportation Security Administration (TSA) considered requiring the use of machine readers on REAL IDs at airports. *At this time* TSA has rejected [the plan]" (emphasis added). Regulatory Evaluation at 58, *supra* note 18.

C. Use of RFID Technology Increases Vulnerability of Data

DHS contemplates using the REAL ID system as part of its Federal border security program and requested comments on how States could incorporate long-range radio frequency identification ("RFID") technology into the REAL ID card so that it could be used as part of the Western Hemisphere Travel Initiative.[78] Many groups have urged against the use of RFID technology in identification documents. There are significant privacy and security risks associated with the use of RFID-enabled identification cards, particularly if individuals are not able to control the disclosure of identifying information. The Department of State recognized these security and privacy threats and changed its E-Passport proposal because of them; the Department of Homeland Security ("DHS") has just abandoned a plan to include RFID chips in border identification documents because the pilot test was a failure; and both the Department of Homeland Security's Data Privacy and Integrity Advisory Committee and the Government Accountability Office recently cautioned against the use of RFID technology in identification documents.

Privacy and security risks associated with RFID-enabled identification cards include "skimming" and "eavesdropping." Skimming occurs when an individual with unauthorized RFID reader gathers information from an RFID chip without the cardholder's knowledge. Eavesdropping occurs when an unauthorized individual intercepts data as it is read by an authorized RFID reader. In the absence of effective security techniques, RFID tags are remotely and secretly readable. Although the creation

[78] REAL ID Draft Regulations at 10,842, *supra* note 1; *see* EPIC, Spotlight on Surveillance, *Homeland Security PASS Card: Leave Home Without It* (Aug. 2006), http://www.epic.org/privacy/surveillance/spotlight/0806/ (why the Western Hemisphere Travel Initiative's proposed passport card creates security threats); EPIC's Page on Radio Frequency Identification (RFID) Systems, http://www.epic.org/privacy/rfid/.

of a small, easily portable RFID reader may be complex and expensive now, it will be easier as time passes. For example, the distance necessary to read RFID tags was initially thought to be a few inches. In the now-abandoned pilot test, the Department of Homeland Security said, "reliable reads can be received from a few inches to as much as 30 feet away from the reader."[79] Other tests also have shown that RFID tags can be read from 70 feet or more, posing a significant risk of unauthorized access.[80]

Some attacks already have succeeded against so-called "strengthened" identification documents. In one case, a computer expert was able to clone the United Kingdom's electronic passport by using a commercially available RFID reader (which cost less than $350) and software that took him less than a couple of days to write.[81] In assessing the new RFID-enabled U.S. passports, one expert cloned the RFID tag and another used characteristics of the radio transmissions to identify individual chips, and those researchers spent only a few weeks attacking the RFID-enabled passports.[82]

Another security risk of RFID-enabled identification cards is that of clandestine tracking. An unauthorized RFID reader could be constructed to mimic the authorized signal and then be used to secretly read the RFID tag embedded in the identification card. The Government Accountability Office has highlighted this security problem unique to wireless technology:

> The widespread adoption of the technology can contribute to the increased occurrence of these privacy issues. As previously mentioned, tags can be read by any compatible reader. If readers and tags become ubiquitous, tagged items

---

[79] Dep't of Homeland Sec., *Notice with request for comments*, 70 Fed. Reg. 44934, 44395 (Aug. 5, 2005), *available at* http://frwebgate1.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=021420363270+2+0+0&WAISaction=retrieve.

[80] *See* Ziv Kfir and Avishai Wool, *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems* (Feb. 22, 2005), *available at* http://eprint.iacr.org/2005/052; Scott Bradner, *An RFID warning shot*, Network World, Feb. 7, 2005.

[81] Steve Boggan, *Special Report: Identity Cards: Cracked It!*, Guardian, Nov. 17, 2006.

[82] Bruce Schneier, Opinion, *The ID Chip You Don't Want in Your Passport*, Wash. Post, Sept. 16, 2006.

> carried by an individual can be scanned unbeknownst to that individual. Further, the increased presence of readers can provide more opportunities for data to be collected and aggregated.[83]

So long as the RFID tag or chip can be read by unauthorized individuals, the person carrying that tag can be distinguished from any other person carrying a different tag. Individuals, unlike commercial products with RFID tags, should have the right to control the disclosure of their identifying information.

The federal government should be fully aware by now of the problems raised by an insecure RFID scheme. In April 2005, EPIC, the Electronic Frontier Foundation, and other groups submitted comments urging the State Department to abandon its E-Passport proposal, because it would have made personal data contained in hi-tech passports vulnerable to unauthorized access.[84] After the Department of State received more than 2,400 comments on its notice for proposed rulemaking on RFID-enabled passports, many of which criticized its serious disregard of security and privacy safeguards, the agency said it would implement Basic Access Control in an attempt to prevent skimming and eavesdropping.[85] The use of RFID-enabled identification documents, without including Basic Access Control and other safeguards, contravenes the Department of State's incorporation of basic security features into new U.S. passports.[86]

In 2005, DHS began testing RFID-enabled I-94 forms in its United States Visitor and Immigrant Status Indicator Technology ("US-VISIT") program to track the entry and

---

[83] Gov't Accountability Office, *Report to Congressional Requesters: Information Security: Radio Frequency Identification Technology in the Federal Government*, GAO-05-551 (May 2005), *available at* http://www.gao.gov/new.items/d05551.pdf.
[84] EPIC, EFF, et. al, *Comments on RIN 1400-AB93: Electronic Passport* (Apr. 4, 2005), *available at* http://www.epic.org/privacy/rfid/rfid_passports-0405.pdf.
[85] Dep't of State, *Notice of Proposed Rule,* 70 Fed. Reg. 8305 (Feb. 18, 2005), *available at* http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-3080.htm.
[86] *See* Kim Zetter, *Feds Rethinking RFID Passport*, Wired, Apr. 26, 2005; Eric Lipton, *Bowing to Critics, U.S. to Alter Design of Electronic Passports*, N.Y. Times, Apr. 27, 2005.

exit of visitors.[87] The RFID-enabled forms stored a unique identification number, which is linked to data files containing foreign visitors' personal data.[88] EPIC warned that this flawed proposal would endanger personal privacy and security, citing the plan's lack of basic privacy and security safeguards.[89] The Department of Homeland Security's Inspector General echoed EPIC's warnings in a July 2006 report. The Inspector General found "security vulnerabilities that could be exploited to gain unauthorized or undetected access to sensitive data" associated with people who carried the RFID-enabled I-94 forms.[90] A report released by the Government Accountability Office in late January identified numerous performance and reliability issues in the 15-month test.[91] The many problems with the RFID-enabled identification system led Homeland Security Secretary Michael Chertoff to admit in Congressional testimony on February 9th that the pilot program had failed, stating "yes, we're abandoning it. That's not going to be a solution" for border security.[92]

---

[87] Dep't of Homeland Sec., *Notice With Request For Comments: United States Visitor and Immigrant Status Indicator Technology Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Border Ports-of-Entry*, 70 Fed. Reg. 44934 (Aug. 5, 2005), *available a*t http://frwebgate1.access.gpo.gov/cgi-∂bin/waisgate.cgi?WAISdocID=021420363270+2+0+0&WAISaction=retrieve.

[88] The data includes biographic information, such as name, date of birth, country of citizenship, passport number and country of issuance, complete U.S. destination address, and digital fingerscans. Dep't of Homeland Sec., *Notice of Availability of Privacy Impact Assessment*, 70 Fed. Reg. 39300, 39305 (July 7, 2005), *available at* http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-13371.htm.

[89] EPIC, *Comments on Docket No. DHS-2005-0011: Notice With Request For Comments: United States Visitor and Immigrant Status Indicator Technology Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Border Ports-of-Entry* (Dec. 8, 2005), *available at* http://www.epic.org/privacy/us-visit/100305_rfid.pdf.

[90] Dep't of Homeland Sec. Inspector Gen., *Additional Guidance and Security Controls Are Needed Over Systems Using RFID at DHS (Redacted)* 7 (July 2006), *available at* http://www.dhs.gov/xoig/assets/mgmtrpts/OIGr_06-53_Jul06.pdf.

[91] Richard M. Stana, Dir., Homeland Sec. & Justice Issues, Gov't Accountability Office, *Testimony Before the Subcom. on Terrorism, Tech., & Homeland Sec., S. Comm. on the Judiciary*, 110th Cong. (Jan. 31, 2007), *available at* http://www.gao.gov/new.items/d07378t.pdf.

[92] Michael Chertoff, Sec'y, Dep't of Homeland Sec., *Testimony at a Hearing on the Fiscal Year 2008 Dep't of Homeland Sec. Budget Before the H. Comm. on Homeland Sec.*, 110th Cong. (Feb. 9, 2007), *available at* http://www.epic.org/privacy/us-visit/chertoff_020907.pdf.

In Congressional testimony in March, a GAO official cautioned against the use of RFID technology to track individuals. "Once a particular individual is identified through an RFID tag, personally identifiable information can be retrieved from any number of sources and then aggregated to develop a profile of the individual. Both tracking and profiling can compromise an individual's privacy," the GAO said.[93] The GAO reiterated the many problems with the failed US-VISIT RFID project and expressed concern that, despite this failure, DHS endorsed the use of RFID in the Western Hemisphere Travel Initiative PASS Card.

In December, the Department of Homeland Security Data Privacy and Integrity Advisory Committee adopted a report, "The Use of RFID for Identity Verification," which included recommendations concerning the use of RFID in identification documents.[94] The committee outlined security and privacy threats associated with RFID similar to the ones discussed below, and it urged against RFID use unless the technology is the "least intrusive means to achieving departmental objectives."[95] It is clear that the RFID technology outweigh its benefits and should not be used in identification documents.

VIII. UNIFORM LICENSE DESIGN WOULD CAUSE DISCRIMINATION AGAINST NON-REAL ID CARDHOLDERS

[93] Linda D. Koontz, Dir., Info. Mgmt. Issues, Gov't Accountability Office, *Testimony Before the Subcom. on Homeland Sec., H. Comm. on Appropriations*, 110th Cong. (Apr. 14, 2007), *available at* http://www.gao.gov/new.items/d07630t.pdf.
[94] Dep't of Homeland Sec., Data Privacy & Integrity Advisory Comm., *The Use of RFID for Human Identity Verification (Report No. 2006-02)* (Dec. 6, 2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf.
[95] *Id.* at 2.

The Department of Homeland Security contemplates a universal design for compliant and non-compliant REAL ID cards.[96] A universal design, especially for a card including citizenship status, would cause irreparable harm, as it would foster suspicion of those who do not wish to carry the REAL ID card. Uniform design for a national identification card would also create an enormous security risk.

A. Universal Design Would Foster Suspicion of Innocent Individuals

The agency is considering a uniform REAL ID card design, asking for comments on "[w]hether DHS should standardize the unique design or color required for non-REAL ID under the REAL ID Act for ease of nationwide recognition, and whether DHS should also implement a standardized design or color for REAL ID licenses."[97] Mandating distinct designs or colors for both REAL ID and regular licenses and identification cards and requiring non-REAL ID driver's licenses or ID cards to have explicit "invalid for federal purposes" designations turns this "voluntary" card into a mandatory national ID card. It would divide the country into two – people with the REAL ID card and those without – and anyone with a different license or ID card would be instantly suspicious. Significant delay, complication and possibly harassment or discrimination would fall upon those who choose not to carry a REAL ID card.

B. Official and Unofficial Purposes of REAL ID Must Not Be Increased

According to DHS, State driver's licenses and identification cards must meet standards set out in the regulations to be accepted for Federal use under REAL ID. Such Federal purposes include entering Federal facilities, boarding commercial aircraft, entering nuclear power plants, and "any other purposes that the Secretary shall

[96] REAL ID Draft Regulations at 10,841-42, *supra* note 1.
[97] *Id.* at 10,842.

determine," but the limitation on use to the three enumerated purposes are "for the time being."[98] The Department of Homeland Security, via the draft regulations and Homeland Security Secretary Michael Chertoff, contemplates expanding the use of the national identification system.

In the draft regulations, the agency seeks comments on "how DHS could expand [the card's official purposes] to other federal activities."[99] In a February speech, Secretary Chertoff said he envisioned the REAL ID licenses "do[ing] double-duty or triple-duty."[100] These national identification cards would "be used for a whole host of other purposes where you now have to carry different identification."[101] The agency also may use the REAL ID card in the Western Hemisphere Travel Initiative program – if citizenship is denoted on the card and long-range RFID technology added.[102]

In the agency's economic analysis of REAL ID implementation, reducing ID theft is listed as one of the potential ancillary benefits of the national identification system. However, the agency says that the potential benefit would depend on a *vast expansion* of REAL ID uses from the three official purposes required in the draft regulations; DHS suggests what is needed is "incidental and required use of REAL ID documents in everyday transactions."[103] DHS envisions that employers, social service agencies

---

[98] Regulatory Evaluation at 30, *supra* note 18.
[99] REAL ID Draft Regulations at 10,823, *supra* note 1.
[100] Michael Chertoff, Sec'y, Dep't of Homeland Sec., *Remarks by Secretary Michael Chertoff at the National Emergency Management Association Mid-Year Conference* (Feb. 12, 2007), *available at* http://www.dhs.gov/xnews/speeches/sp_1171376113152.shtm.
[101] *Id*.
[102] *See* RFID Technology discussion, *supra* Section VII(c) (security and privacy risks inherent in RFID use), and Citizenship Designation discussion, *supra* Section IV (citizenship designation breeds discrimination).
[103] Regulatory Evaluation at 130, *supra* note 18; *see* Identity Theft discussion, *infra* at Section X(c) (why REAL ID will not reduce identity theft).

(including Medicare, Medicaid and student financial aid), firearm sellers and licensors, and election workers will all use this national identification system.[104]

The official and unofficial uses of REAL ID must not be broadened. Such expansion would harm national security. As explained below, using a single card for many identification purposes would be the same as using one key for every lock.

IX. EXPANDED DATA COLLECTION AND RETENTION INCREASES SECURITY RISKS

Under REAL ID, the government would have easy access to an incredible amount of personal data stored in one national database (or, according to the DHS description, 56 State and Territory databases, each of which can access all of the others).[105] DHS claims that it is not expanding data collection and retention, but it is enlarging schedules and procedures for retention and distribution of identification documents and other personal data. This broad expansion of data collection and retention in a national database creates significant threats to privacy and security.

The agency makes two claims about the expanded data retention under REAL ID that we dispute: (1) "Most States already include this [extensive, personal] information in a machine readable technology," and (2) "neither the Real ID Act nor these proposed regulations gives the Federal Government any greater access to information than it had before."[106] Each claim is false: DHS is mandating the increase of both the type of documents that need to be retained and the length of data retention, and the agency will give both State and Federal governments greater access to the personal data.

---

[104] *See* National Committee for Voting Integrity, http://votingintegrity.org/ *and* EPIC, Spotlight on Surveillance, *With Some Electronic Voting Systems, Not All Votes Count* (Sept. 2006), http://www.epic.org/privacy/surveillance/spotlight/0307 (why requiring any voter identification card is a poll tax).
[105] Section 202(d)(12); (d)(13).
[106] REAL ID Draft Regulations at 10,824, *supra* note 1.

With the REAL ID national identification system, DHS imposes new requirements on State motor vehicle agencies. Each of the 56 interconnected databases must contain all data fields printed on driver's licenses and ID cards, and driver's histories, including motor vehicle violations, suspensions, and points on licenses.[107] The States are compelled to begin maintaining paper copies or digital images of important identity documents, such as birth certificates or naturalized citizenship papers, for seven to 10 years.[108] This is a significant expansion of the personal data previously reviewed or stored by State motor vehicle agencies.

Currently these identification documents are kept in a variety of places – the Social Security system, the immigration system, local courthouses – and it takes considerable effort to gather them all together. Under REAL ID, all of these identification documents – concerning, among other things, births, marriages, deaths, immigration, social services – are consolidated into one national database, accessible to at least tens of thousands of government employees nationwide, which would give the Federal and State governments greater access than before.

Security expert Bruce Schneier, EPIC and others have explained that it decreases security to have one ID card for many purposes, as there will be a substantial amount of harm when the card is compromised.[109] There is also the threat that REAL ID is ostensibly trying to protect against: forged identification cards. Investing so much trust into one card means that criminals will only have to forge one identification card. "No

[107] Section 202(d)(12); (d)(13).
[108] REAL ID Draft Regulations at 10,855, *supra* note 1.
[109] Melissa Ngo, Dir., EPIC Identification & Surveillance Project, *Prepared Testimony and Statement for the Record at a Hearing on "Maryland Senate Joint Resolution 5" Before the Judicial Proceedings Comm. of the Maryland Senate* (Feb. 15, 2007) ["EPIC Testimony at Maryland Senate"], *available at* http://www.epic.org/privacy/id_cards/ngo_test_021507.pdf.

matter how unforgeable we make it, it will be forged. We can raise the price of forgery, but we can't make it impossible. Real IDs will be forged," Schneier said.[110] A national database full of identification documents, images and data would entice many kinds of criminals, including terrorists who seek to steal the identity of a "trusted" individual.

A national identification system would divide the United States into two groups: (1) "trusted good guys" who have the national ID card, and (2) "untrusted bad guys" who do not. But, Schneier has pointed out that there is a third category that appears – bad guys who fit the good guy profile. Upon the release of the draft regulations, Schneier said, "The REAL ID regulations do not solve problems of the national ID card, which will fail when used by someone intent on subverting that system. Evildoers will be able steal the identity – and profile – of an honest person, doing an end-run around the REAL ID system."[111] This national identification system inherently contains significant threats to individual privacy and national security.[112]

X. NATIONAL ID DATABASE WOULD INCREASE SECURITY VULNERABILITIES

In the best-case scenario, the creation of the REAL ID national identification system does nothing to improve our security protections. In the worst-case scenario, the REAL ID system will exponentially increase threats to our national security. DHS's cryptic economic analysis is based upon incredible assumptions about possible future terrorist attacks that REAL ID would supposedly prevent. The economic analysis also ignores indirect costs. The REAL ID system would harm national security by increasing

[110] Bruce Schneier, *Real-ID: Costs and Benefits,* BULLETIN OF ATOMIC SCIENTISTS, Mar./Apr. 2007 ["Schneier Essay"], *available at* http://www.schneier.com/blog/archives/2007/01/realid_costs_an.html.
[111] Press Release, EPIC, After Long Delay, Homeland Security Department Issues Regulations For Flawed National ID Plan (Mar. 2, 2007), *available a*t http://www.epic.org/press/030207.html.
[112] *See* National Database discussion, *supra* Section X (how universal identification systems increase security threats).

risks of identity theft and fraud, and by diverting funds away from other security programs that have been proven effective.

A. Regulations Would Not Improve Our Security Protections

Quantitative risk assessments are characteristically limited by false or unverifiable assumptions, faulty modeling, and above all short-sighted local optimization that tends to ignore long-term implications and slippery-slope changes in the validity of the assumptions.[113] The economic analysis in the Department of Homeland Security's Regulatory Evaluation conducts such a quantitative risk assessment, and falls victims to these faulty assumptions. The Regulatory Evaluation states:

> The primary benefit of REAL ID is to incrementally increase U.S. national security by reducing the vulnerability to criminal or terrorist activity of federal buildings, nuclear facilities, and aircraft. The chances of a terrorist attack on such targets being successful would generally increase if identity documents that grant access to them are in the possession of the attackers. This is demonstrated by the fact that several of the 9/11 hijackers had false driver's licenses or fraudulently obtained driver's licenses in their possession at the time of that attack.[114]

The analysis goes on to say, "REAL ID is highly unlikely to impact the consequences of a successful attack, but it may impact, on the margin, the chance of a terrorist attack being attempted and succeeding."[115] So, DHS is attempting to determine the marginal chance that REAL ID will lessen the chance of success or discourage the attempt of a terrorist attack. Setting aside the assumption that a lack of REAL ID cards would make it more difficult to succeed in a terrorist attack upon the United States, we turn to the mathematical formula that DHS uses to calculate the REAL ID system's presumed "primary benefit."

---

[113] Peter G. Neumann, *Computer-Related Risks*, § 7.10, Risks in Risk Analysis, pp. 255-257(Addison-Wesley 1995).
[114] Regulatory Evaluation at 126, *supra* note 18.
[115] *Id*. at 127.

> The annual risk that the U.S. faces with regard to a potential terrorist attack can be represented as the chance that an attack will successfully take place, multiplied by the consequences of that attack. This can be mathematically represented as ∏*K, where ∏ is the annual chance of a successful attack and K is the consequences of an attack in monetary terms. Homeland security measures such as REAL ID impact either the chance or consequences of a successful attack, or both. REAL ID is highly unlikely to impact the consequences of a successful attack, but it may impact, on the margin, the chance of a terrorist attack being attempted and succeeding. Let ∏B be this chance prior to the introduction of REAL ID, and □A be the chance after REAL ID comes into effect. Then the security impact of REAL ID in the course of one year can be measured in dollar terms as (∏B – ∏A)*K.[116]

So, DHS takes the probability of a successful terrorist attack without the REAL ID national identification system in place (□B) and **subtracts** the probability of a successful attack with REAL ID (□A); then they take the resulting number and **multiply it by** the cost to the United States of a successful terrorist attack. Understandably, DHS goes onto explain that such an evaluation is very difficult and full of uncertainty.

> Let the cost of the REAL ID regulation, which has been estimated, be C. Then for REAL ID to be fully justified on national security grounds alone, it must be the case that its benefit is at least as great as its costs. The annual risk-reduction benefit of Real ID is (∏B – ∏A)*K, and the sum of this benefit over ten years must equal Real ID's cost, C. If we can determine a dollar value for K, then we can measure the marginal impact that REAL ID must bring about on the probability of a successful terrorist attack on a federal target for it to be fully justified by its security benefit.[117]

DHS is attempting to determine if (∏B – ∏A)*K, which is the annual risk-reduction benefit of REAL ID, over 10 years, is at least equal to C, which is the cost of REAL ID, which DHS has set at – a discounted rate of – $17.2B. DHS goes on to explain that this formula is based on the assumption that another attack would affect us, in economic terms, the same as September 11, 2001. DHS estimates another attack would cost the United States either $63.9 billion (an estimate of the immediate impact incurred) or

[116] *Id*. at 127.
[117] *Id*.

$374.7B (an estimate of the immediate and longer run impact).[118] Other assumptions:

> We assume that terrorist groups are seeking to inflict another attack with consequences on the order of magnitude of 9/11. We also assume that they are engaged in a campaign such that in every year during the 10-year period over which the costs and benefits of REAL ID are being evaluated, there is a positive and identical probability of being successfully attacked. Under this assumption, the expected present value of the consequences of the terrorist campaign against the U.S. homeland equals the sum of the expected values of consequences in each particular year over the 10-year period 2007-16:
>
> ∏2007*K2007 + (1-∂)*□2008*K2008 + (1-∂)2*□2009*K2009 + ... + (1-∂)9*∏2016*K2016,
>
> where □ is the discount rate and K is the monetary value of consequences in real 2006 dollars. Because we assume that □ and □ do not change from year to year, this can be re-written as:
>
> ∏*K + (1-∂)* ∏*K + (1-∂)2* ∏*K + ... + (1-∂)9* ∏*K ,
>
> or
>
> D*∏*K, where D equals {1 + (1-∂) + (1-∂)2 + ... + (1-∂)9}.
>
> This expression is the sum of the expected discounted annual consequences of a terrorist campaign against the U.S. homeland over a ten-year period. As noted earlier, Real ID is anticipated to bring about a reduction in the annual probability of a successful attack from ∏B – ∏A, and the security benefit of Real ID over the ten-year period is therefore D*(∏B – ∏A)*K.[119]

The variable D represents the annual consequences of a terrorist campaign against the U.S. over a ten-year period. DHS **multiplies D by** [(∏B – ∏A) times K], which is the annual risk-reduction benefit of REAL ID. DHS then sets this equation **equal to** the direct cost of the REAL ID national ID system. By solving this equation, DHS hopes to find the **marginal impact on security** that the REAL ID system must have in order to **break even**. For "Real ID to break even with respect to cost and expected security

[118] *Id*. at 127.
[119] Regulatory Evaluation at 128-29, *supra* note 18.

benefits, it must be the case that D*(∏B – ∏A)*K = C, or ∏B – ∏A = C/(D*K)."[120] So, to break even, we need [D*(∏B – ∏A)*K] **to be equal to** C, meaning that how much REAL ID will save us in economic terms must be equal to the cost of the REAL ID system. Or, stated another way, it must be that ∏B – ∏A, probability of a successful terrorist attack without the REAL ID national identification system in place (□B) **minus** the probability of a successful attack with REAL ID (∏A), **is equal to** C, cost of REAL ID system, **divided by** [D, annual consequences of a terrorist campaign against the U.S. over a ten-year period, multiplied by K, cost to the United States of a successful terrorist attack].

Here is where it gets tricky. Assuming the cost of REAL ID to be $17.2B and the cost of a successful 9/11-type terrorist attack to be $374.7 billion long-term, the value of C/D*K, in 2006 dollars, is 0.61%. Therefore, for "REAL ID to be fully justified by its primary security benefit, it must bring about a marginal reduction in the annual chance of a successful 9/11-type attack of 0.61%."[121] If DHS only estimates the immediate impact, and assumes the cost of REAL ID to be $17.2 billion and the cost of the attack to be $63.9 billion, then the value of C/(D*K) is 3.60%. "For REAL ID to be fully justified by its primary security benefit in immediate impacts alone, it must bring about a marginal reduction in the annual chance of a successful 9/11-type attack of 3.60%."[122]

After all of these head-scratching mathematical assumptions, there is no conclusion, because, as DHS explains, "[w]ithout further information on the absolute level of □B [the probability of a successful terrorist attack without the REAL ID national identification system in place], it is difficult to say whether 0.61% or 3.60% is a very large reduction in

[120] *Id*. at 129.
[121] *Id*.
[122] *Id*.

the chance of successful attack, or a more moderate reduction."[123] Therefore, it is unknown, even with all of these assumptions, whether REAL ID would even marginally reduce the possibility of a successful terrorist attack.

DHS acknowledges that certain assumptions are used in this analysis, such as assumptions for the variable K, the impact or the cost to the U.S. economy of a terrorist attack, which DHS assumes would be of the same magnitude as September 11, 2001. However, there is little discussion about the variable C, the cost of the REAL ID system. There are two ways in which the figures used by DHS are faulty: 1) they underestimate the direct costs and 2) they ignore the indirect costs. Such indirect costs include the impact upon civil liberties, increased risk of identity theft and fraud, and the diversion of funds from other, effective security programs.[124] Both faulty assumptions make the variable C smaller, while DHS has assumed a very large number for K, so the cost of the REAL ID system would seem dwarfed in comparison to the cost of another terrorist attack, making REAL ID seem cost-effective even if it only has a marginal effect on the probability of another attack – an effect REAL ID would not have.

REAL ID does not add to our security protections, but in fact increases our security threats by diverting needed funds from other national security projects. The estimated cost of REAL ID implementation has spiraled. Before the Act's passage in 2005, the Congressional Budget Office estimated its cost to be around $100 million.[125] In September, the National Conference of State Legislatures released a report estimating the

[123] *Id.*
[124] *See* Identity Theft discussion, *infra* at Section X(c) (REAL ID increases risks for identity theft).
[125] Cong. Budget Office, *Cost Estimate: H.R. 418: REAL ID Act of 2005* (Feb. 9, 2005), *available at* http://www.cbo.gov/showdoc.cfm?index=6072&sequence=0&from=6.

cost to be $11 billion over the first five years.[126] Now, the Department of Homeland Security has admitted that REAL ID will cost states and individuals from $17.2 billion to $23.1 billion over ten years.[127] Congress has appropriated only $40 million for REAL ID implementation. The Department of Homeland Security now says that a state can use up to 20 percent of its Homeland Security Grant Program funding for REAL ID implementation, which total about $100 million for 2007.[128] Implementation costs for the state of California alone would be about $500 million.[129]

Diverting Homeland Security Grant Program money to REAL ID means that funding originally budgeted by the states for other homeland security projects, including training and equipment for rescue and first responder personnel. Even if the states received $100 million per year for 10 years, that would still amount to only $1.04 billion in Federal funds, a fraction of the $17.2 billion to $23.1 billion price tag. The rest of the cost would be borne by states and their residents.

B. Regulations Would Increase National Security Threats

In a recent analysis of the REAL ID Act, EPIC Executive Director Marc Rotenberg explained that "[s]ystems of identification remain central to many forms of security. But designing secure systems that do not introduce new risks is proving more difficult than many policymakers had imagined."[130] The theory that the REAL ID Act

[126] Governors' Analysis, *supra* note 46.
[127] REAL ID Draft Regulations at 10,845, *supra* note 1.
[128] Press Release, Dep't of Homeland Sec., DHS Issues Proposal for States to Enhance Driver's Licenses (Mar. 1, 2007), *available at* http://www.dhs.gov/xnews/releases/pr_1172765989904.shtm.
[129] Cal. Dep't of Motor Vehicles, *Report to the Legislature on the Status of the REAL ID Act*, at 3 (Dec. 15, 2006), *available at* http://www.dmv.ca.gov/about/real_id/real_id.pdf.
[130] Marc Rotenberg, Exec. Dir., EPIC, *Real ID, Real Trouble?*, COMMUNICATIONS OF THE ACM, Mar. 2006, *available at* http://www.epic.org/privacy/id_cards/mr_cacm0306.pdf.

will prevent terrorism is predicated on the belief that only "outsiders" have an intent to harm the United States. This theory is fundamentally flawed.

Security expert Bruce Schneier has explained the theory of identification-based security. "In theory, if we know who you are, and if we have enough information about you, we can somehow predict whether you're likely to be an evildoer," Schneier said.[131] This is impossible, because you cannot predict intent based on identification, he said.[132] There are threats from both sides. Terrorist acts have been committed by U.S. citizens, "insiders." Oklahoma City bombers Timothy McVeigh and Terry Nichols were U.S. citizens. As was Unabomber Ted Kaczynski.

A recent case illustrates Schneier's point. According to court documents, last month, two men entered restricted areas at an airport in Florida, bypassed security screeners and carried a duffel bag containing 14 guns and drugs onto a commercial plane."[133] They avoided detection, because they are airline baggage handlers who used their uniforms and legally issued identification cards.[134] Both men had passed Federal background checks before they were hired, according to a spokesman for Comair, the airline that employed the men.[135] This questions the assumption that more and broader background checks, such as those suggested in the draft regulations, would prevent insider attacks. There are other problems with the background checks, which will be discussed below.[136]

---

[131] Schneier Essay, *supra* note 110.
[132] *Id.*
[133] Jim Ellis, *Feds: Bag Of Guns Smuggled Onto Plane*, Associated Press, Mar. 9, 2007.
[134] *Id.*
[135] *Id.*
[136] *See* Domestic Violence discussion, *infra* Section XI.

The baggage handlers were only investigated and caught after police received an anonymous tip.[137] If the airport had identification-neutral security systems, such as requiring all fliers go through metal detectors, then the men could not have walked past them. But the identification-based security system failed because it allowed some fliers to skip screening because they are presumed to have no evil intent, and the men transported weapons and contraband aboard a commercial flight. Creating a national identification system would have just as devastating consequences, but on a larger scale, because many more people would be presumed "trusted" or "untrusted" based upon their decision to carry or not carry the REAL ID card.

C. Even If Assumptions Granted, REAL ID Would Not Substantially Affect Identity Theft Crimes

The draft regulations list reducing identity theft as one of the benefits of the REAL ID national identification system.[138] However, the agency's own economic analysis under its Regulatory Evaluation shows that, even if one grants DHS the economic assumptions it makes, overall identity theft crimes would only be reduced by 2.8 percent, at best.[139]

First, it is important to note that the DHS Regulatory Evaluation does not list "Reduce Identity Theft" under any of the three categories of benefits – "monetized," "annualized quantified, but unmonetized," or "unquantifiable benefits" in the accounting statement for the draft regulations.[140] Actually, the only benefit listed is under "unquantifiable benefits," and that is the claim that REAL ID would "incrememental ly increase U.S. national security."

---

[137] Jim Ellis, *Feds: Bag Of Guns Smuggled Onto Plane*.
[138] REAL ID Draft Regulations at10,837, 10,846, *supra* note 1.
[139] Regulatory Evaluation at 5, *supra* note 18.
[140] *Id*. at 7.

Second, the Regulatory Evaluation later lists "reducing identity theft" as a potential ancillary benefit.[141] The economic analysis explains that:

> REAL ID will only have the ability to impact those types of identity theft that require a drivers license for successful implementation, and only to the extent that the rulemaking leads to incidental and required use of REAL ID documents in everyday transactions, which is an impact that also depends critically on decisions made by State and local governments and the private sector.[142]

The potential ancillary benefit depends on a *vast expansion* of REAL ID uses from the three official purposes required in the draft regulations. The economic analysis assumes that REAL ID would be used in "everyday transactions," which would have a devastating affect on identity theft protections.[143] Setting aside that flawed assumption and focusing upon the economic analysis, there is little benefit to be found. If all of the agency's assumptions are agreed to, including the belief that REAL ID cards would be used in everyday transactions, the Department of Homeland Security still finds that REAL ID would reduce by 10 percent only the 28 percent of ID theft crimes that "are likely to require the presentation of an identity document like a drivers license."[144] Therefore, the REAL ID national identification system will reduce only 2.8 percent of all identity theft crimes, a savings of approximately $1.6 billion total for the 2007-2016 period.[145] The Department of Homeland Security has estimated that REAL ID would cost $23.1 billion for that period. Basic economic analysis finds that one ought not spend $23.1 billion to create a national identification system that might reduce the cost of identity theft crimes by $1.6 billion.

---

[141] *Id*. at 126, 129-30.
[142] *Id*. at 130.
[143] *See* Identity Theft discussion, *infra* at Section X(c) (REAL ID increases risks of identity theft).
[144] Regulatory Evaluation at 130, *supra* note 18.
[145] *Id*.

D. Centralized Identification System Increases Risk of Identity Theft

The draft regulations create a national identification system with a national database, and this creates an enormous security risk. EPIC and others have explained that it decreases security to have a centralized system of identification, one ID card for many purposes, as there will be a substantial amount of harm when the card is compromised.[146]

The REAL ID Act mandates that States provide every other state with electronic access to information contained in their motor vehicle databases and each State database must contain all data fields printed on driver's licenses and ID cards, and driver's histories, including motor vehicle violations, suspensions, and points on licenses.[147] Yet, DHS claims that a national database will not be created because the regulations "leave[] the decision of how to conduct the exchanges in the hands of the States."[148] This mandatory "State-to-State data exchange" creates one huge national database containing the personal information of 245 million license and ID cardholders – a database that can be accessed at DMVs across the country.

Using a national ID card would be as if you used one key to open your house, your car, your safe deposit box, your office, and more.[149] "The problem is that security doesn't come through identification; security comes through measures – airport screening, walls and door locks – that work without relying on identification"; therefore,

---

[146] EPIC Testimony at Maryland Senate, *supra* note 109; *see* EPIC, *Comments to the Federal Identity Theft Task Force, P065410* (Jan. 19, 2007), *available at* http://www.epic.org/privacy/idtheft/EPIC_FTC_ID_Theft_Comments.pdf; EPIC page on Identity Theft: Its Causes and Solutions, *available at* http://www.epic.org/privacy/idtheft/.

[147] Section 202(d)(12); (d)(13).

[148] REAL ID Draft Regulations at 10,825, *supra* note 1.

[149] Melissa Ngo, Dir., Identification & Surveillance Project, EPIC, *Prepared Testimony and Statement for the Record at a Meeting on "REAL ID Rulemaking" Before the Data Privacy & Integrity Advisory Comm., Dep't of Homeland Sec.* (Apr. 14, 2007), *available at* http://www.epic.org/privacy/id_cards/ngo_test_032107.pdf.

a centralized system of identification would not increase national security, security expert Bruce Schneier has said.[150]

A large data breach affects the confidence and trust of the public. People will recoil from systems that create privacy and security risks for their personal data. We have seen countless data breaches that have left the personal data of tens of millions of Americans vulnerable to misuse. Recently, almost 46 million credit and debit card numbers were stolen by hackers who accessed the computer systems at the TJX Companies over a period of several years, making it the biggest breach of personal data ever reported.[151] The computer system breaches began in July 2005 but weren't discovered until December 2006 – the financial data of millions were exposed for 17 months.[152] Last May, an information security breach by a Department of Veterans Affairs employee resulted in the theft from his Maryland home of unencrypted data affecting 26.5 million veterans, active-duty personnel, and their family members.[153] The laptop and an external hard drive contained unencrypted information that included millions of Social Security numbers, disability ratings and other personal information.[154] In February 2005, databroker Choicepoint sold the records of at least 145,000 Americans to a criminal ring engaged in identity theft.[155] Also that year, Bank of America misplaced back-up tapes

---

[150] Press Release, EPIC, After Long Delay, Homeland Security Department Issues Regulations For Flawed National ID Plan (Mar. 2, 2007), *available at* http://www.epic.org/press/030207.html.
[151] TJX Cos., Annual Report (Form 10-K), at 8-10 (Mar. 28, 2007), *available at* http://ir.10kwizard.com/download.php?format=PDF&ipage=4772887&source=487.
[152] *Id*. at 7.
[153] *See* EPIC's Page on the Veterans Affairs Data Theft, http://www.epic.org/privacy/vatheft/.
[154] Statement, Dep't of Veterans Affairs, A Statement from the Department of Veterans Affairs (May 22, 2006).
[155] Robert O'Harrow Jr., *ID Theft Scam Hits D.C. Area Residents*, Wash. Post, Feb. 21, 2005, at A01; *see* EPIC's Page on ChoicePoint, http://www.epic.org/privacy/choicepoint/.

containing detailed financial information on 1.2 million employees in the Federal government, including many members of Congress.[156]

A centralized identification system would be a tempting target for identity thieves. If a criminal breaks the system's security, then the criminal would have access to the personal information of every single person in that database. If this one, centralized system is used across the nation, this would put hundreds of millions of people at risk for identity theft.

There is another significant security risk, besides that of attacks by unauthorized users, and that is of authorized users abusing their power.[157] A 2005 scandal in Florida highlights risks associated with large database systems. A woman wrote to a newspaper criticizing a Florida sheriff as being too fat for police work and condemning his agency's use of stun guns.[158] Orange County Sheriff Kevin Beary ordered staffers to use state driver's license records to find the home address of his critic.[159] The sheriff sent her a letter at her home address, and she reported being surprised that he was able to track her down so easily.[160] In a case in Maryland just last year, three people – including a Maryland Motor Vehicle Administration official – were indicted on charges of "conspiring to sell unlawfully produced MVA-issued Maryland identification cards."[161]

The consumer harm that results from the wrongful disclosure of personal information is very clear. For the seventh year in a row, identity theft is the No. 1 concern

---

[156] Robert Lemos, *Bank of America loses a million customer records*, CNet News.com, Feb. 25, 2005.
[157] *See* Domestic Violence discussion, *infra* Section XI (abusers use their authorized access to stalk victims).
[158] *Called fat, sheriff tracks down reader*, Associated Press, Apr. 6, 2005.
[159] *Id.*
[160] *Id.*
[161] *Fake ID Cards*, Wash. Post, Mar. 15, 2006, at B02.

of U.S. consumers, according to the Federal Trade Commission's annual report.[162] Over 104 million data records of U.S. residents have been exposed due to security breaches since January 2005, according to a report from the Privacy Rights Clearinghouse.[163] A centralized system of identification creates a "one-stop shop" for identity thieves. Centralizing authority over personal identity into one database and one card increases both the risk of identity theft as well as the scope of harm when it occurs. The confidence and trust of consumers will fall when such a breach occurs; people will withdraw because of privacy and security questions.

XI. REAL ID HARMS VICTIMS OF DOMESTIC VIOLENCE AND SEXUAL ASSAULT

The REAL ID national identification system creates difficulties for many groups, and it has significant consequences for domestic violence and sexual assault victims.[164] The residential address requirements endanger the ability of victims of domestic violence, sexual assault, and other crimes to hide from their abusers. The background check provisions set out in the draft regulations do not fully protect these victims from their abusers. In fact, the REAL ID system would help abusers find and track their victims across the nation.

A. REAL ID Endangers Address Confidentiality

Currently, many States allow domestic violence victims and others to protect the confidentiality of their residential addresses. States have created formal Address Confidentiality Programs and states have also provided general measures of residential

[162] Fed. Trade Comm'n, *Consumer Fraud and Identity Theft Compliant Data: January – December 2006* (Feb. 7, 2007), *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.
[163] Privacy Rights Clearinghouse, Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm.
[164] *See* EPIC's Page on REAL ID and Domestic Violence, http://www.epic.org/privacy/dv/real_id.html.

address privacy. The proposed regulations override these substantial protections, and the overrides must be removed from the final regulations. The government must not make it easier for abusers to find their victims.

State Address Confidentiality Programs are an important tool for protecting the safety of domestic violence and sexual assault victims. Currently 20 states have address confidentiality programs.[165] Generally, under such programs, domestic violence or sexual assault victims register with the secretary of State or their attorney general. The victim is provided an address with that State office, which forwards the mail received there to the enrollee's residential address. This State office address is used in official correspondence with the State, though businesses are not usually required to use it.

The REAL ID Act requires that driver's licenses include a person's "address of principal residence."[166] This requirement effectively destroys state address confidentiality programs. The recent Violence Against Women and Department of Justice Reauthorization Act ("VAWA") included a requirement for DHS to "consider and address" the needs of certain groups when the agency is "developing regulations or guidance with regard to identification documents, including driver's licenses,"[167] These groups include domestic violence and sexual assault victims who are entitled to be enrolled in State address confidentiality programs; whose addresses are entitled to be suppressed via court order or State or Federal law; or whose information is protected

[165] *See*, Nat'l Conference of State Legislatures, *States With Address Confidentiality Programs for Domestic Violence Survivors,* http://www.ncsl.org/programs/cyf/dvsurvive.htm (listing 19 states, not including Maryland but including Illinois which is unfunded); *See also*, Maryland Safe At Home Address Confidentiality Program, http://www.sos.state.md.us/ACP/Information.htm.
[166] Pub. L. No. 109-13, § 202(b)(6), 119 Stat. 231, 312 (2005).
[167] Pub. L. No. 109-162, § 827, 119 Stat. 2960, 3066 (2005).

from disclosure according to Section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act 1996.[168]

In the draft regulations, DHS has not followed the VAWA requirement; instead, the agency has significantly reduced the protections afforded by these programs. The proposed regulations require that addresses of principal residence be placed on the face of the REAL ID card and include some exemptions from this requirement, such as one for those enrolled in Federal Witness Security Programs.[169] The regulations also exempt those who are enrolled in State address confidentiality programs.[170] This is not the same as creating an exemption for those who are "entitled to be enrolled in the programs, as stated under the Violence Against Women Act." In its discussion of the proposed rule, DHS does propose to include an exemption for those who are "entitled to be enrolled" in state address confidentiality programs.[171] DHS must include this exemption in the final regulations. It cannot be that, as currently stated under the draft regulations, only those actually enrolled in State Address Confidentiality Programs would be exempted from the requirement to display their residential addresses on the face of the REAL ID card. Many domestic violence and sexual assault victims who are entitled to enroll in State Address Confidentiality Programs are not actually enrolled, for a variety of personal, safety and logistical reasons. They should not be punished for not actually enrolling in the program.

In order to adequately "consider and address" the needs of those who are "entitled to be enrolled" in a State confidentiality program, DHS must permit States to allow those who are entitled to be, but are not in address confidentiality programs to be exempted

---

[168] Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, § 827, 119 Stat. 2960, 3066 (2005).
[169] REAL ID Draft Regulations at 10854, *supra* note 1.
[170] *Id*. at 10854.
[171] *Id*. at 10836.

from the address of principal residence requirement. DHS should allow individuals to affirm that they fear victimization and would benefit from address confidentiality. It would be problematic to burden State motor vehicle agencies with the determination of who is entitled to be enrolled in an address confidentiality program. States could rely on the affirmation, rather than making a determination of the merits of an individual's need for confidentiality. This would close the gap between those domestic violence and sexual assault victims who are "entitled to be enrolled" and those who are actually enrolled in State Address Confidentiality Programs.

Also, though the proposed rule exempts from the residential address requirement those whose addresses are "entitled to be suppressed under State or Federal law or suppressed by a court order," this statement should be clarified to include States that generally allow individuals to display on licenses and ID cards an address other than their principal place of residence.[172] Several States generally allow non-residential addresses to be on driver's licenses. Currently, at least seven States permit an address other than a residential address to be listed on licenses or ID cards (California,[173] Florida,[174] Montana,[175] New Mexico,[176] Oklahoma,[177] Wyoming,[178] and Virginia[179]). For example, under Virginia's law, an applicant may choose to list a post office box, business or residential address.[180] The applicant is still required to provide their residential address

[172] REAL ID Draft Regulations at 10854, *supra* note 1.
[173] Cal. Veh. Code § 12811(a)(1)(A).
[174] Fla. Stat. Ann. § 322.14(1)(a).
[175] Mont. Code. Ann. § 61-5-111.
[176] N.M. Stat. Ann. § 66-5-15 (1978).
[177] Okla. Stat. Ann. tit. 47, § 6-111(A)(1).
[178] Wyo. Stat. Ann. § 31-7-115(a)(iii).
[179] Va. Code Ann. § 46.2-342(A1).
[180] *Id*.

for motor vehicle department records, but this residential address is not displayed on the license or ID card.[181]

Domestic violence survivors, other crime victims, or those generally interested in protecting their privacy avail themselves of these State laws to keep their addresses confidential. These laws are the only way that survivors can protect themselves in States that do not have formal address confidentiality programs – four of those listed do not (Montana, New Mexico, Virginia and Wyoming). These general address privacy laws are also the only way that those who fear victimization, but who do not formally qualify for State Address Confidentiality programs, can protect themselves.

Without this exemption allowing States to permit any individual to protect her privacy by listing a non-residential address, the victims of domestic violence and sexual abuse will also face the embarrassment of disclosing that they are victims anytime that their identification is shown. There are few exceptions from the residential address requirement, and anyone holding a REAL ID card without the residential address listed would immediately be placed into one of these few categories.

B. National Database Threatens Security of Victims of Abuse Crimes

The draft regulations require that States provide electronic access to their motor vehicle database information to all other States.[182] Survivors who flee their abusers, crossing into different states, will be exposed if their abuser breaches the security of any one of these interconnected databases. An abuser with an associate inside a State DMV, law enforcement, or other agency with access to the State records would be able to track a victim as the victim moves across the country.

---

[181] *Id.*

[182] REAL ID Draft Regulations at 10,856, *supra* note 1.

The danger of negligent and accidental disclosures is increased by REAL ID, as substantially more government employees will have access to all motor vehicle records nationwide. One example of accidental disclosure occurred in Wisconsin earlier this year -- a police officer disclosed a victim's address, found in a DMV record to a stalker; the officer did not know that the victim had a restraining order against this.[183] This sort of inadvertence would happen much more frequently in a post-REAL ID world, as access to personal information is spread throughout the national identification system. Intentional breaches by outsiders or authorized insiders abusing their power would also have a wider scope. Past abuses exemplify what can be expected in a nationwide scale. For example, in Arizona, a police officer admitted to accessing motor vehicle records to find personal information on women he was romantically interested in, as well as co-workers.[184] If REAL ID is implemented, abusers and insiders would have access to records throughout the country and would be able to track their victims no matter where they flee.

C. Proposed Background Check Procedures Do Not Fully Protect Victims of Abuse Crimes

DHS proposes that certain government employees be subject to criminal history background checks, with certain offenses disqualifying employees from specific jobs related to the REAL ID national identification system.[185] Covered employees would be limited to those who could affect the recording of information, the manufacture of REAL ID cards, or the information displayed on a card.[186] Employees who can access the record information without the ability to edit it are not subject to the background check

[183] Kevin Murphy, *Officer's Actions will Cost 25,000*, GAZETTEXTRA, Feb. 15, 2007, *available at* http://www.gazetteextra.com/mezera021507.asp.
[184] Michael Kiefer, *Officer Admits to Tampering; Databases Used to Check on Women*, ARIZONA REPUBLIC, April 6, 2006, at B3.
[185] REAL ID Draft Regulations at 10,855, *supra* note 1.
[186] *Id*. at 10,856.

requirement. This massive loophole greatly increases the security and privacy risks of domestic violence and sexual abuse victims, as significant damage can be done by unauthorized data disclosure. In order to safeguard against these threats, the broad category of those who have access to records should be shrunk, rather than increasing the category of those who are covered by the background check requirement.

The suitability criteria of the background check do not match the threat of stalkers and abusers. DHS proposes to use the permanent and interim disqualifying criteria in the Transportation Security Administration's background checks for maritime and land transportation security at 49 C.F.R. 1572.103.[187] The offenses include espionage, sedition, treason, making bomb threats, and crimes involving transportation security incidents.[188] Some of the offenses, such as fraud and misrepresentation -- including identity fraud -- are relevant to the risks of improper disclosure and access to the records.[189] However, crimes such as stalking, surveillance, harassment and domestic abuse are not in this list. These crimes must be added to the list of disqualifying offenses, so that the REAL ID system does not create a loophole permitting abusers access to a national database that would allow them to track their victims no matter where the victims moved.

D. REAL ID Increases the Power Abusers Have Over Their Victims

REAL ID's stringent document requirements will place more power in the hands of abusers. Fleeing domestic violence or sexual abuse can be a sudden and dramatic step. Victims' advocates often counsel their clients to prepare "safety plans," which include

[187] *Id*. at 10,856.
[188] 49 C.F.R. 1572.103(a).
[189] *Id*. at 1572.103(b)(2)(iii).

gathering key documents such as passports, visas, and birth certificates.[190] The proposed regulations limit the types of documents that can be used to prove identity, which create problems for many groups, including abuse victims.[191] The draft regulations permit exceptions for those who do not have the required documents "for reasons beyond their control."[192] The exception requires that the records "visibly indicate" that alternative documentation was accepted and that a "full explanation" of the reason be included in the record.[193] Thus victims will face the embarrassment of having intimate details of the abuse they have suffered included in a national database accessible to thousands of government employees across the nation. The "for reasons beyond their control" exception must specifically include abuse victims, so that they may not be punished for leaving their abusers. The visible indication and "full explanation" included in the records should be limited to the statement that alternative documents were accepted "for reasons of personal safety," so that victims need not expose the history of their abuse to anyone who could view their DMV records.

Another problem is that this "for reasons beyond their control" exception does not apply to those who must demonstrate lawful immigration status.[194] Under the draft regulations, the demonstration of lawful status would require documents that an abuser would likely have control over. Abusers of immigrants who are able to control their victims immigration documents will be able to control the victim's ability to obtain a

---

[190] *E.g.*, Oakland County Coordinating Council Against Domestic Violence, *Domestic Violence Handbook – Personalized Safety Plan*, *at* http://www.domesticviolence.org/plan.html (last visited Mar. 30, 2007) ("Items to take, if possible. . . Birth Certificates . . . Social security cards . . . Passports, green cards, work permits").
[191] REAL ID Draft Regulations at 10,852, *supra* note 1; *see* Data Verification discussion, *supra* Section VI (general problems with the standards).
[192] REAL ID Draft Regulations at 10,852, *supra* note 1.
[193] *Id.*
[194] *Id.*

REAL ID card or license. The "for reasons beyond their control" exception must be extended to those victims who must prove lawful immigration status, so that the abusers cannot use these documents to trap their victims into staying in abusive situations. The exception permitting those who do not have access to documents to use alternative documentation should be extended to the proof of lawful immigration status. Here, also, the visible indication and "full explanation" included in the victims' DMV records should be limited to the statement that alternative documents were accepted "for reasons of personal safety," so that victims need not expose the history of their abuse to anyone and everyone who could view their DMV records.

XII. METASYSTEM OF IDENTIFICATION IS BETTER CHOICE

Once personal data has fallen into the hands of an identity thief, the potential for its misuse is proportionate to the extent that the information can be used for illegitimate authentication. We have already explained why a universal identifier will not improve security. Rather than promoting the use of universal identifiers, EPIC advocates the distribution of identity or an identity metasystem in which authentication is confined to specific contexts in order to limit the scope for potential misuse. The danger of a single identifier is that the harm will be magnified when it is compromised.

A system of distributed identification reduces the risks associated with security breaches and the misuse of personal information. For example, a banking PIN number, in conjunction with a bank card, provides a better authentication system because it is not coupled with a single, immutable consumer identity. If a bank card and PIN combination is compromised, a new bank card and PIN number can be issued and the old combination cancelled, limiting the damage done by the compromised data. Drawbacks of such

structures, including the possibility for the existence of multiple cards, are currently being addressed by the creation of an identity metasystem in which multiple identities can be loosely coupled within a single secure system.[195]

Distributing identity in this way allows for different profiles to be used in different authenticating contexts. New profiles can be created as required within a single identity metasystem. Misuse is therefore limited to the context of the information breached, whether it is a single bank account, online merchant, or medical records.

Possibilities for data misuse can also be limited at the data collection stage. EPIC has previously called attention to the need for Web sites to stop storing customer credit card information.[196] Amassing large databases of credit card numbers creates an attractive target for potential identity thieves. Creating a national ID card under REAL ID also creates an attractive target for potential identity thieves – imagine having access to digital copies of "breeder" documents, such as certified birth certificates and SSN cards.

First and foremost, the best response is not to create a centralized identification system such as the one realized under REAL ID. Another simple response to identity theft is to require a PIN to be used in conjunction with all identification cards. A third response is to forbid third-party collection or storage of data from identification cards. An identity metasystem would further reduce the value of such aggregated database targets, because authenticators would be separate and distinct from all personally identifiable information.

Finally, technological measures can be used to improve the reliability of authentication while respecting consumer privacy. International research efforts are

[195] Kim Cameron, *The Laws of Identity*, Identity Weblog, Dec. 9, 2004, http://www.identityblog.com/stories/2004/12/09/thelaws.html.
[196] *See* EPIC's Page on Identity Theft: Causes and Solutions, http://www.epic.org/privacy/idtheft/.

currently underway to create authentication systems that preserve anonymity, and include the development of new privacy enhancing technologies for use in such schemes.[197] These privacy enhancing technologies allow for the separation of authentication and identification and are being deployed in response to security vulnerabilities. Such technologies may plug in to identity metasystems, such as Microsoft's CardSpace. While the default settings of CardSpace do not currently meet recognized standards for privacy preservation,[198] this model should be studied in detail.[199]

XIII. IMPLEMENTATION JUST NOT POSSIBLE UNDER CURRENT TIMELINE

Two years after Congress rushed through passage of the REAL ID Act, the Department of Homeland Security announced on March 1 proposed regulations to create the REAL ID national identification system. The draft regulations were released about 14 months before the May 2008 implementation deadline. After enormous criticism from the public and the States, DHS extended the deadline, but not by much.

Comments on the draft regulations are due by May 8. DHS says it will review the public comments and take them into consideration for the final regulations, the release of which is expected in August or September.[200] In the draft regulations, DHS says it

---

[197] *See, e.g.*, Carlisle Adams, *Delegation and Proxy Services in Digital Credential Environments*, Presented at the 7th Annual Privacy and Security Workshop, *Your Identity Please: Identity Theft and Identity Management in the 21st Century* (Nov. 2, 2006), *available at* http://www.idtrail.org/files/cacrwkshpdigcred02nov06.pdf; Stefan Brands, *Non-Intrusive Cross-Domain Digital Identity Management*, Presented at Proceedings of the 3rd Annual PKI R&D Workshop (Apr. 2004), *available at* http://www.idtrail.org/files/cross_domain_identity.pdf; David Chaum, *Secret-Ballot Receipts: True Voter-Verifiable Elections*, Presented at ITL Seminar Series*, Secret-Ballot Receipts: True Voter-Verifiable Elections*, Nat'l Inst. of Standards & Tech. (May 19, 2004); Paul Van Oorschot and S. Stubblebine, *Countering Identity Theft through Digital Uniqueness, Location Cross-Checking, and Funneling*, Fin. Cryptography & Data Sec. (2005), *available at* http://www.scs.carleton.ca/~paulv/papers/pvoss6-1.pdf.

[198] Stefan Brands, *User centric identity: boon or worst nightmare to privacy?*, Identity Corner, Nov. 17, 2006, http://www.idcorner.org/?p=142.

[199] *See generally*, NAT'L RESEARCH COUNCIL, WHO GOES THERE? AUTHENTICATION THROUGH THE LENS OF PRIVACY (Nat'l Academies 2003).

[200] DHS Testimony at REAL ID Hearing, *supra* note 11.

"strongly encourages States to submit certification packages by October 1, 2007," and sets a drop-dead date of February 10, 2008, for states to file these certification packages, which detail States' plans to fulfill the obligations detailed in the final regulations.[201] These certification packages include a "comprehensive security plan for [each State's] DMV offices and driver's license storage and production facilities, databases, and systems utilized for collecting, disseminating or storing information used in the issuance of REAL ID licenses."[202] This comprehensive security plan must also include "how the State will protect the privacy of the data collected, used, and maintained in connection with REAL ID, including all the source documents."[203] The certification packages must also include an exceptions process for people who cannot fulfill the requirements necessary to receive a REAL ID card.[204]

The two-year delay in releasing draft regulations and the short timeline for the States to create "certification packages" detailing how they will comply with the final regulations makes it virtually impossible for the States to create useful implementation plans that take privacy and security questions into consideration. This fast-track scheduling makes it appear dubious that DHS will take comments submitted by the public into account when creating the final regulations for REAL ID implementation, though the agency is required to under law.

XIV. REAL ID MUST BE REPEALED

REAL ID is fundamentally flawed because it creates a national identification system. It cannot be fixed no matter what the implementation regulations say. Therefore,

[201] REAL ID Draft Regulations at 10,824, *supra* note 1.
[202] *Id*. at 10,825.
[203] *Id*. at 10,825.
[204] *Id*. at 10,822.

the REAL ID Act must be repealed. Federal legislation has been introduced to repeal the REAL ID Act.[205] Arkansas, Maine, Idaho, Montana, and Washington State all have passed legislation rejecting the REAL ID Act, and more than 20 other states are debating similar legislation.[206]

The Department of Homeland Security protests that it must implement the REAL ID Act, but Homeland Security Secretary Michael Chertoff has worked with members of Congress in the past on problems with implementing the REAL ID Act.[207] He can continue to work with members of Congress to reject this national identification scheme.

XV. CONCLUSION

For the foregoing reasons, the Coalition urges the Department of Homeland Security to recommend to Congress that REAL ID is unworkable and must be repealed. The REAL ID Act creates an illegal *de facto* national identification system filled with threats to privacy, security and civil liberties and undermines well-established principles of law found in the Privacy Act. Assuming that REAL ID is repealed, any subsequent legislation should be subjected to extensive review that explicitly addresses all of the issues raised in this document.

Respectfully submitted,

ELECTRONIC PRIVACY INFORMATION CENTER

---

[205] *See* EPIC's page on National ID Cards and the REAL ID Act page, http://www.epic.org/privacy/id_cards/ (information about federal and state legislation concerning REAL ID).

[206] *Id*.

[207] At the press conference announcing the release of the draft regulations for REAL ID implementation, Secretary Chertoff said, "And, I want to say in particular that in formulating the proposal that we're announcing today we were delighted to work closely with governors and members of Congress." Michael Chertoff, Sec'y, Dep't of Homeland Sec., Remarks at a Press Conference on REAL ID (Mar. 1, 2007), transcript *available at* http://www.dhs.gov/xnews/releases/pr_1172834392961.shtm.

AND

[EXPERTS IN PRIVACY AND TECHNOLOGY]

STEVEN AFTERGOOD
PROF. ANITA ALLEN
PROF. ANN BARTOW
PROF. JAMES BOYLE
DAVID CHAUM
SIMON DAVIES
WHITFIELD DIFFIE
PROF. DAVID FARBER
PHILIP FRIEDMAN
DEBORAH HURLEY
PROF. JERRY KANG
CHRIS LARSEN
MARY MINOW
DR. PETER G. NEUMANN
DR. DEBORAH PEEL
STEPHANIE PERRIN
PROF. ANITA RAMASASTRY
BRUCE SCHNEIER
ROBERT ELLIS SMITH
PROF. DANIEL J. SOLOVE
PROF. FRANK M. TUERKHEIMER