

epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

**REAL ID IMPLEMENTATION REVIEW:
FEW BENEFITS, STAGGERING COSTS**

ANALYSIS OF THE DEPARTMENT OF HOMELAND SECURITY'S
NATIONAL ID PROGRAM

ELECTRONIC PRIVACY INFORMATION CENTER

MAY 2008

**REAL ID IMPLEMENTATION REVIEW:
FEW BENEFITS, STAGGERING COSTS**

ANALYSIS OF THE DEPARTMENT OF HOMELAND SECURITY'S
NATIONAL ID PROGRAM

ELECTRONIC PRIVACY INFORMATION CENTER

MAY 2008

About EPIC

The Electronic Privacy Information Center is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.

EPIC staff

Marc Rotenberg
President & Executive Director

Lillie Coney
Associate Director & Coordinator, The Privacy Coalition

Melissa Ngo
Senior Counsel & Director, EPIC Identification & Surveillance Project

John Verdi
Staff Counsel & Director, EPIC Open Government Project

Katitza Rodríguez Pereda
Director, EPIC International Privacy Project & Coordinator, The Public Voice

Simon Davies
Senior Fellow

Harry Hammitt
Senior Fellow

Guilherme Roschke
Skadden Fellow

Daniel Burger
Administrative Director

Acknowledgements

For support of our efforts to safeguard privacy and civil liberties in the post-9/11 era, EPIC gratefully acknowledges the contributions of individual donors and the following foundations: the Ford Foundation, the Fund for Constitutional Government, the HKH Foundation, the Irving Kohn Foundation, the Albert List Foundation, the OSI, the Rockefeller Family Fund, the Scherman Foundation, the Sun Hill Foundation, and the Trio Foundation of St. Louis.

EXECUTIVE SUMMARY

Throughout its history, the United States has rejected the idea of a national identification system. Yet, the Department of Homeland Security continues to push forward a system of identification that has been widely opposed. The REAL ID Act mandates that State driver's licenses and ID cards follow federal technical standards and verification procedures issued by Homeland Security. REAL ID also enables tracking, surveillance, and profiling of the American public.

May 11, 2008 was the statutory deadline for implementation of the REAL ID system, but not one State is in compliance with the federal law creating a national identification system. In fact, 19 States have passed resolutions or laws rejecting the national ID program. The Department of Homeland Security has faced so many obstacles that the agency now plans an implementation deadline of 2017 -- nine years later than the 2008 statutory deadline.

Homeland Security claims that it is making strides in implementing the national ID program. Homeland Security Secretary Michael Chertoff encourages the use of the REAL ID system for a wide variety of purposes unrelated to the law that authorized the system. In an opinion column written by Secretary Chertoff after the publication of the final rule in January, he said, "embracing REAL ID" would mean it would be used to "cash a check, hire a baby sitter, board a plane or engage in countless other activities." None of these uses for the REAL ID have a legal basis. Each one creates a new risk for Americans who are already confronting the staggering problem of identity theft.

Last year, EPIC submitted detailed comments to the DHS on the draft proposal for REAL ID. With the assistance of many experts, we attempted to address the enormous challenge in the project proposal. In the following report, EPIC details the many problems with the final plan to implement this vast national identification system. The REAL ID system remains filled with threats to privacy, security and civil liberties that have not been resolved.

MARC ROTENBERG
EPIC EXECUTIVE DIRECTOR

MELISSA NGO
DIRECTOR, EPIC IDENTIFICATION
& SURVEILLANCE PROJECT*

* EPIC Skadden Fellow Guilherme Roschke contributed to this report.

TABLE OF CONTENTS

I. INTRODUCTION: HISTORY OF NATIONAL IDENTIFICATION	1
II. THE CREATION OF THE REAL ID SYSTEM	3
A. REAL ID Is Still Not Voluntary	4
B. Standards for ID Documents Remain Burdensome for Many	5
C. REAL ID’s Data Verification Procedures Still Based on Faulty Premises.....	7
III. HOMELAND SECURITY HAS ABDICATED ITS RESPONSIBILITY TO PROTECT INDIVIDUAL PRIVACY.....	10
A. Unfettered Access to 2D Barcode Data Threatens Individual Privacy	12
B. REAL ID Increases Both Insider and Outsider Threats.....	14
C. Background Check Procedures Fail to Address Insider Threat Problems	16
D. Final Rule Includes Marginal Improvements for Address Confidentiality and Name History Problems.....	17
IV. REAL ID SYSTEM CREATES NEW NATIONAL SECURITY RISKS.....	18
V. STATES OPPOSE NATIONAL ID SYSTEM.....	20
VI. RECOMMENDATION: DECENTRALIZE IDENTIFICATION	22
VII. CONCLUSION	23
APPENDIX I. STATE LEGISLATION AGAINST REAL ID ACT.....	24
APPENDIX II. EPIC EXPERT COMMENTS ON DRAFT REAL ID REGULATIONS	25

I. INTRODUCTION: HISTORY OF NATIONAL IDENTIFICATION

National identification cards have long been advocated as a means to enhance national security; unmask potential criminals, chiefly terrorists; and guard against illegal immigration.¹ The cards are used in many countries including Belgium, Egypt, France, Germany, Greece, Hong Kong, Malaysia, and South Africa.² Currently, the United States and the United Kingdom continue to debate the merits of adopting national ID cards. The types of card, their functions, and privacy safeguards vary widely.

EPIC and Privacy International's *Privacy and Human Rights: An International Survey of Privacy Laws and Developments*, explains the basics of the technology used in national ID cards:

In recent years technology has rapidly evolved to enable electronic record creation and the construction of large commercial and State databases. A national identifier contained in an ID card enables disparate information about a person that is stored in different databases to be easily linked and analyzed through data mining techniques. ID cards are also becoming "smarter" – the technology to build microprocessors the size of postage stamps and put them on wallet-sized cards has become more affordable. This technology enables multiple applications such as a credit card, library card, health care card, driver's license and government benefit program information to be all stored on the same national ID along with a password or a biometric identifier.³

During the history of the national ID card debate in the United States, Americans have consistently rejected the creation of such a 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.⁴ Though use of the SSN has expanded considerably, it is not a universal identifier and efforts to make it one have been consistently rejected. In 1971, the Social Security Administration task force on the Social Security Number⁵ declined to transform the number into an ID card.⁶ The Health, Education and Welfare Secretary's Advisory Committee on Automated Personal Data Systems in 1973 again rejected the creation of a national identifier and advocated the establishment of significant safeguards to protect personal data. The committee said:

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

The Federal Advisory Committee on False Identification also advised against the use of a national identifier in 1976.⁸ In 1977, the Privacy Protection Study Commission recommended against the adoption of a national ID system.⁹ In its report, *Personal Privacy in an Information Society*, the commission said that it:

sees a clear danger that a government record system, such as that maintained by the Social Security Administration or the Internal Revenue Service, will become a *de facto* central population register unless prevented by conscious policy decisions. Therefore [...] the Federal government should act positively to halt the incremental drift toward creation of a standard universal label and central population register until laws and policies regarding the use of records about individuals are developed and shown to be effective.¹⁰

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.”¹¹ The Clinton administration advocated a “Health Security Card” in 1993 and assured the public that the card, issued to every American, would have “full protection for privacy and confidentiality.”¹² Still, the idea was rejected and the card never was created. In 1999, Congress repealed a controversial provision in the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 that authorized the inclusion of SSNs on driver’s licenses.¹³

In response to the tragic events of September 11, 2001, there has been renewed interest in the creation of national ID cards. Soon after the attacks, Larry Ellison, head of California-based software company Oracle Corporation, called for the development of a national identification system and offered to donate the technology to make this possible. He proposed ID cards with embedded digitized thumbprints and photographs of all legal residents in the U.S.¹⁴ There was much public debate about the issue, and Congressional hearings were held. Former House Speaker Newt Gingrich testified that he “would not institute a national ID card because you do get into civil liberties issues.”¹⁵ Congress, in establishing the Department of Homeland Security, expressly prohibited the agency from developing National ID systems.¹⁶ The Act stated simply:

Nothing in this Act shall be construed to authorize the development of a national identification system or card.¹⁷

Nonetheless, the Department of Homeland Security continues to push forward with the REAL ID plan, as well as other proposals for identification and tracking.¹⁸

II. THE CREATION OF THE REAL ID SYSTEM

In May 2005, the REAL ID Act was appended to a bill providing tsunami relief and military appropriations and passed with little debate and no hearings.¹⁹ It was passed in this manner 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.²⁰ The senators said they believe “Legislating in such a complex area without the benefit of hearings and expert testimony is a dubious exercise and one that subverts the Senate’s deliberative process.”²¹ Even though Congress was unable to debate the matter, civil liberties organizations began a public dialogue shortly after passage of the REAL ID Act.²²

When the agency released the draft regulations in March 2007, it received more than 21,000 public comments.²³ EPIC joined 24 experts in privacy and technology in submitting comments that detailed significant privacy and security problems in the draft regulations.²⁴ EPIC also encouraged public participation in the rulemaking process through a project organized by the Privacy Coalition, and in collaboration with over 60 organizations and more than 200 Internet bloggers.²⁵

On January 11, 2008, about two and a half years after the passage of the REAL ID Act of 2005, Department of Homeland Security Secretary Michael Chertoff released the final rule to implement the national identification system created under the Act.²⁶ The proposal has drawn sharp criticism from State governments,²⁷ members of Congress,²⁸ civil liberties advocates,²⁹ and security experts.³⁰

In response to the public comments to the draft regulations, the Department of Homeland Security scaled back some of the requirements, reduced the cost, and extended the deadline for State compliance in the final rule for the REAL ID system.³¹ However, Secretary Chertoff continues to encourage the use of the REAL ID system for a wide variety of purposes unrelated to the law that authorized the system, including employment eligibility verification.³² He also indicates that the agency would not prevent the use of the card by private parties for non-government purposes.³³ Also, as part of the cost-saving effort, Homeland Security decided not to encrypt the data that will be stored on the card.³⁴

Though the Department of Homeland Security made some modification and attempted to solve several problems described in the public comments, the changes are not enough. REAL ID remains unworkable and should be repealed. The Department of Homeland Security is attempting to create 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.

Even if REAL ID implementation were to go forward, the final regulations include poor privacy and security safeguards for the sensitive personal data of cardholders. The changes made in response to public comments about the proposed draft regulations are marginal, at best. For such a system to have the minimum protections necessary, the requirements of the Privacy Act of 1974 must be fully enforced for all uses of the data, current and future.³⁵ Agencies should not be permitted to assert any exemptions, and individuals must be granted all rights, including the judicially enforceable right to access and correct their records and to ensure compliance with all Privacy Act requirements. Moreover, technical safeguards need to be incorporated into both the identity card and the databases systems. The DHS failed to establish adequate safeguards for privacy and security.

In our May 2007 comments to Department of Homeland Security concerning the draft REAL ID regulations, EPIC listed several privacy and security problems inherent in this national identification scheme. Below, we detail how the final regulations have changed the REAL ID system and whether our criticisms were answered.

A. *REAL ID Is Still Not Voluntary*

The Department of Homeland Security has repeatedly stated that REAL ID is not mandatory, therefore, it is not an unfunded mandate. However, in EPIC's May 2007 comments on the draft REAL ID regulations, we explained the reasons why REAL ID is not a "voluntary" program. "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."³⁶ Also, "The administration has also pursued a heavy-handed assault on those who have raised legitimate questions about the efficacy, cost, and impact of the [REAL ID] program. [. . .] 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.' "³⁷

In the final rule, the Department of Homeland Security does nothing to change this initial assessment. In fact, the REAL ID initiative has practically invited proposals for expanded identification requirements in the United States.³⁸ Though the agency limited the "official purposes" of REAL ID cards to the

statutorily mandated purposes (“boarding of Federally-regulated commercial aircrafts, entering of Federal facilities, and nuclear power plants”), the agency said it “will continue to consider additional ways in which a REAL ID license can or should be used.”³⁹ In its discussion of the final rule, DHS also said “widespread” acceptance of the REAL ID national identification system could lead to restrictions in “access to public subsidies and benefits programs” as well as restricting access to firearms or even elections.⁴⁰ In his remarks announcing the final rule, DHS Secretary Michael Chertoff said that “it is probably reasonably predictable that as these licenses become more widely distributed,” then more groups will choose to use REAL ID cards; in fact, he said they would likely “flock” to the REAL ID national identification system.⁴¹

The Department of Homeland Security continues its assault against States that contemplate rejection of the REAL ID national identification system. In the discussion of the final rule, the agency said it “believes that many States may find noncompliance an unattractive option” because the States would not be able to “maintain the conveniences enjoyed by their residents when using their State-issued driver’s licenses and non-driver identity cards for official purposes, particularly as it pertains to domestic air travel.”⁴²

“That will mean real consequences for their citizens starting in May if their leadership chooses not to comply,” Department of Homeland Security spokeswoman Laura Keehner said in January.⁴³ “That includes getting on an airplane or entering a federal building, so *they will need to get passports.*” (emphasis added).⁴⁴ This is a significant monetary penalty, as U.S. passports currently cost \$85 to \$100.⁴⁵ DHS itself admits that only “25% of the population already holds a valid passport.”⁴⁶

EPIC’s assessment concerning the “voluntary” nature of the REAL ID national identification system remain unchanged from May. The Department of Homeland Security’s declared support for and expectation of “widespread” use of the REAL ID systems, and the agency’s continued pressure on the States and penalties for noncompliance prove the involuntariness of the national identification program.

B. Standards for ID Documents Remain Burdensome for Many

Under the REAL ID Act, States are required to obtain and verify documents from applicants that establish “(A) A photo identity document, except that a non-photo identity document is acceptable if it includes both the person’s full legal name and date of birth. (B) Documentation showing the person’s date of birth. (C) Proof of the person’s social security account number or verification that the person is not eligible for a social security account number. (D) Documentation showing the person’s name and address of principal residence” and “Evidence of lawful status.”⁴⁷ Though DHS has made minimal

changes to the standards for identity documents that REAL ID applicants must provide, the agency has not solved the problems EPIC detailed in the May 2007 comments.

Under the final 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; (2) certified copy of a birth certificate; (3) consular report of birth abroad; (4) unexpired permanent resident card; (5) unexpired employment authorization document; (6) unexpired foreign passport with valid U.S. visa affixed and “the approved I-94 form documenting the applicant’s most recent admittance into the United States”; (7) U.S. certificate of naturalization; (8) U.S. certificate of citizenship; or (9) REAL ID driver’s license or identification card issued in compliance with the final regulations.⁴⁸ Notably, in the final regulations, the agency “has added a provision that would allow DHS to change the list of documents acceptable to establish identity following publication of a notice in the Federal Register.”⁴⁹ Therefore, the Department of Homeland Security could make the identification document requirements even more burdensome at a later date.

These documents are virtually unchanged from those listed in the draft regulations, and such difficult standards for acceptable identification documents would limit the ability of some individuals to get a State driver’s license. As we explained in May 2007, “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.”⁵⁰ We noted that the Department of Homeland Security attempted to resolve this problem by allowing the States to voluntarily create an exceptions process for extraordinary circumstances, but “though DHS set minimum standards for data collection, retention and documentation of the transaction, the agency did not set minimum standards for eligibility, length of process, or cost of process.”⁵¹

The document requirements create specific problems for domestic violence victims. Under the draft regulations, the demonstration of lawful status would require documents that an abuser would likely have control over.⁵² Abusers of immigrants who are able to control their victims’ immigration documents will be able to control the victim’s ability to obtain a REAL ID card or license. EPIC urged the Department of Homeland Security to extend exceptions 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. We also recommended that 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.

The REAL ID final rule is a little more sensitive to the problems of immigrant victims of domestic abuse. In the final rule, there is no requirement that records visibly indicate alternative documentation or that “full explanations” be attached when the exceptions process is invoked.⁵³ The Department of Homeland Security also indicates that simple explanations such as “for reasons of public safety” or other “generic expressions” may be used.⁵⁴ The exceptions process is also extended to allow determination of lawful status in the case of U.S. citizenship, but not other status.⁵⁵ However, the Department of Homeland Security leaves unaddressed the problem of immigrant women whose abusers destroy, steal or otherwise control their documents.

Also problematic is that, in the final rule, DHS explicitly removed the only substantive guidance it detailed on the exceptions process. In the draft regulations, DHS stated that persons born before 1935 might not have been issued birth certificates, so they might be eligible for the exceptions process.⁵⁶ But in the final rule, DHS removes this eligibility exemption.⁵⁷ In the final regulations, there is nothing that explains to either States or individuals how REAL ID applicants could prove eligibility (other than that the “process may not be used by non-citizens to establish lawful status in the United States”),⁵⁸ how long the process would take (days, weeks, months or even years), or if applicants could even afford the cost of the exceptions process, which would be above and beyond the already-high cost of the REAL ID card.

C. REAL ID’s Data Verification Procedures Still Based on Faulty Premises

In EPIC’s May 2007 comments, we detailed specific problems with the draft regulations’ data verification procedures, including, 1) DHS relies on verification databases that are not available, 2) of the databases that are available, some are not widely available, 3) of the databases that are available, government and independent analyses have proven (and the Department of Homeland Security itself has admitted) that there the information in these databases are incomplete or full of errors), and 4) State DMV employees are unable and should not be forced to become federal immigration officials.⁵⁹ The final regulations promulgated by the Department of Homeland Security do not adequately address these problems.

Beyond the national identification system created by the State-to-State data exchange, two of four verification systems required are not fully deployed nationwide and third does not even exist. 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) an as-yet uncreated Department of State system “to verify

passports, U.S. visas, and other information held by the Department of State," such as Consular Reports of Birth, and Certifications of Report of Birth.⁶⁰

When the draft regulations were released, the only system that was 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.⁶¹ SSOLV depends on data gathered in a system whose mistakes are well-known, the Numerical Identification File ("NUMIDENT").⁶² The Social Security Administration's Inspector General estimated that about 17.8 million records in the NUMIDENT have discrepancies with name, date of birth or death, or citizenship status.⁶³ About 13 million of these incorrect records belong to U.S. citizens.⁶⁴

Federal reviews have found such data "seriously flawed in content and accuracy."⁶⁵ In an October opinion granting a temporary restraining order enjoining the Department of Homeland Security from implementing a new "no-match" employment eligibility verification proposal, the federal judge noted "the government recognizes, the no-match letters are based on SSA records that include numerous errors."⁶⁶ In the final rule, Department of Homeland Security admits there are accuracy and reliability problems in SSOLV said that it, AAMVA, and the States are working with SSA to attempt to solve these problems.⁶⁷

In the draft regulations, DHS revealed "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 implementation deadline of May 2008."⁶⁸ Now, Department of Homeland Security claims "a majority" of States are enrolled in SAVE, but that it is still "working to modify the system" so that States can use it to implement the REAL ID national identification system.⁶⁹ The agency also says that the planned connection between SAVE and SEVIS has not been completed.⁷⁰

EVVE is currently in pilot phase and only 11 States are participating, an increase of six more than the five States that were participating in May 2007.⁷¹ In the draft regulations, the Department of Homeland Security based its requirements on the assumption that EVVE would be ready for nationwide expansion by the implementation deadline of May 11, 2008.⁷² Now, DHS admits, "the EVVE system is not ready for full implementation. The final rule provides for additional time for States to implement EVVE or another system that provides for the verification of birth records."⁷³ DHS burdens the States by requiring that the States either use a system that the agency admits is not ready

for full deployment or the States themselves must create such a complex and costly system.

In the draft regulations, DHS required that the States use a State Department system to verify passports and some reports of births that was not yet created. The agency based this mandate on the assumption that the system “is eventually developed.”⁷⁴ In the final rule, DHS admits the system still does not exist and says it is working “to provide a capability to verify passports, U.S. visas, and other information held by the Department of State.”⁷⁵

DHS states in the final rule that “States cannot and will not be required to use systems that are not fully operational and available for use,” yet the agency then details mandates for the States to use systems that are not fully operational and available for use.⁷⁶ It is clear that the agency has not solved the significant problems with its verification databases and has ensured that even States that wish to implement REAL ID will confront substantial obstacles and may not be able to do so.

There is a further problem with the revised verification procedures: the Department of Homeland Security anticipates that State DMV employees will become Federal immigration officials.⁷⁷ The Department of Homeland Security has not adequately addressed these problems in its final rule for the implementation of the REAL ID national identification system.

Under the final rule, State DMV employees would still be required to verify REAL ID national identification card applicants’ source documents. DHS defined “verification” as “two interrelated procedures: (1) inspection to see if the document is genuine and has not been altered, and (2) checking to see that the identity data on the document is valid.”⁷⁸

Under the final regulations, the source documents that would be accepted by the States to issue these new identity cards would be: (1) valid unexpired U.S. passport; (2) certified copy of a birth certificate; (3) consular report of birth abroad; (4) unexpired permanent resident card; (5) unexpired employment authorization document; (6) unexpired foreign passport with valid U.S. visa affixed and “the approved I-94 form documenting the applicant’s most recent admittance into the United States”; (7) U.S. certificate of naturalization; (8) U.S. certificate of citizenship; or (9) REAL ID driver’s license or identification card issued in compliance with the final regulations.⁷⁹ As we noted above, in the final regulations, the agency “has added a provision that would allow DHS to change the list of documents acceptable to establish identity following publication of a notice in the Federal Register.”⁸⁰ Therefore, the document verification requirements could become even more burdensome for State DMV employees.

State DMV employees would be required to verify these source documents, including Federal immigration documents, though this is a complex and confusing area of law. In the draft regulations, DHS sought to solve this problem by requiring that DMV employees handling source documents undergo 12 hours of “fraudulent document recognition” training.⁸¹ The final rule mandates “Fraudulent document recognition training for all covered employees handling source documents or engaged in the issuance of driver’s licenses and identification cards.”⁸²

A Government Accountability Office review of the Social Security Administration found that staff had difficulty recognizing counterfeit documents, though it is their primary job to verify these documents before issuing Social Security numbers.⁸³ For example, the Government Accountability Office 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.”⁸⁴

We reiterate what we said in our May 2007 comments, “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 [...] when it is difficult for counterfeit documents to be spotted by federal employees whose primary job is verification of source documents.”⁸⁵ It still remains unclear would happen if a State DMV employee determines that an applicant’s source documents are fraudulent: What recourse would the applicant have to prove her documents are real? In the final regulations, the Department of Homeland Security again has punted its Privacy Act obligations, including appropriate redress procedures.

III. HOMELAND SECURITY HAS ABDICATED ITS RESPONSIBILITY TO PROTECT INDIVIDUAL PRIVACY

The Department of Homeland Security has stated that it is constrained in its power to protect the privacy of individuals and their data under the REAL ID Act. The agency claimed in the draft regulations that, “The Act does not include statutory language authorizing DHS to prescribe privacy requirements for the state-controlled databases or data exchange necessary to implement the Act.”⁸⁶ We agree with Sen. Joseph Lieberman, who said, “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.”⁸⁷

The final 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. The agency has the obligation to protect the privacy of individuals affected by this system and must do more than the feeble attempts set out in the draft regulations.

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.⁸⁸ 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.”⁸⁹ 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.”⁹⁰ The REAL ID system is operated under a Federal mandate to accomplish several agency functions, including immigration control.

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, “DHS Information Systems” is defined 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.”⁹¹ 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.⁹²

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. The final regulations conclude that individuals should attempt to exercise their rights to notice, access, correction and redress through State DMVs, the Social Security Administration, the Department of State, and the U.S. Citizenship and Immigration Service (a part of the Department of Homeland Security).⁹³

Once again, the Department of Homeland Security has punted the issue of privacy to the States, but the agency needs to lead. Various questions remain, including important ones concerning 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 Privacy Act protections must be mandated in the REAL ID implementation regulations in order for the Department of Homeland Security to fulfill its obligations.

A. Unfettered Access to 2D Barcode Data Threatens Individual Privacy

There are significant threats to individual privacy and security that would be created by unfettered access to REAL ID national identification system data.⁹⁴ Some of the problems are based on the design of the card and the safeguards for the underlying databases. Though the Department of Homeland Security has made some changes in the final rule, substantial problems remain.

Under REAL ID, the following data elements, 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 issuance and expiration dates.⁹⁵ The REAL ID card will include a 2D barcode as its machine-readable technology, which will include elements 1 through 7 and 10, with these notations, "(b) Full legal name, unless the State permits an applicant to establish a name other than the name that appears on a source document, pursuant to Sec. 37.11(c)(2)"; "(f) Address as listed on the card pursuant to Sec. 37.17(f)"; "(h) Card design revision date, indicating the most recent change or modification to the visible format of the driver's license or identification card"; "(i) Inventory control number of the physical document"; and, "(j) State or territory of issuance."⁹⁶

We support the Department of Homeland Security in its rejection of radio frequency identification (RFID) technology as the machine-readable technology for the REAL ID national identification card. Multiple reports, including the recommendations of the Department's own Data Privacy and Integrity Advisory Committee, made clear that RFID should not be used for human identification.⁹⁷ However, the Department's decision to leave the 2D barcode unencrypted creates unnecessary security risks.⁹⁸ In doing so, the Department of Homeland Security rejects the advice of independent privacy and security experts and the agency's own Privacy Office. The DHS 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.⁹⁹

There are many examples of unauthorized users being able to download data from unencrypted machine-readable technology.¹⁰⁰ One case involved New York prosecutors charging 13 people with harvesting data from unencrypted, machine-readable credit cards and clubs downloading all data contained on unencrypted State licenses.¹⁰¹ To protect privacy and improve security, this machine-readable technology must either include encryption or access must be limited in some other form. As we explained earlier, “Leaving the machine readable zone open would allow unfettered third-party access to the data and leave 245 million license and cardholders nationwide at risk for individual tracking.”¹⁰²

The Department of Homeland Security rejected encryption in the final rule because of “the complexities and costs of implementing an encryption infrastructure.”¹⁰³ We anticipated this and detailed a privacy-protective alternative to encryption, yet the agency did not take this path either. We said:

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.¹⁰⁴

Instead of accepting this simple, privacy-protective suggestion, the Department of Homeland Security chose to require that a great deal of personal data be stored on the 2D barcode.

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.”¹⁰⁵ The agency has this obligation and it should not abdicate this responsibility. 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 data for purposes beyond the three official purposes.

Rejecting encryption for the 2D barcode helps to push the REAL ID system into “widespread” use in everyday life, a goal that DHS Secretary

Chertoff and the DHS final rule itself expect and support. Such an expansion would harm both individual privacy and security and quickly turn the United States into a country where the REAL ID national identification card is involuntarily carried by everyone.

B. REAL ID Increases Both Insider and Outsider Threats

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 final regulation from Department of Homeland Security, 56 State and Territory databases, each of which can access all others through a “hub”-based network).¹⁰⁶ As it did in the draft regulations, in the final regulations 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 Department of Homeland Security justifies the expanded data collection on the misleading representations that 1) “most States” already gather, retain and distribute such extensive personal data and documents, and 2) the REAL ID national identification system does not give States or the Federal government greater access to sensitive personal data and documents than before.¹⁰⁷ The REAL ID national identification system mandates increased data gathering, retention and distribution, as well as massively expanding the Federal and State access to this data. The personal data of 245 million State license and ID cardholders would be accessible from a massive number of DMVs across the country.

Consolidating identity through a single document increases risks when the document is compromised. It would be as if you used one key to open your house, your car, your safe deposit box, your office, and more.¹⁰⁸ “Perversely – a harder-to-forge card makes subverting the system even more valuable. Good security doesn’t try to divine intentionality from identification, but instead provides for broad defenses regardless of identification,” such as airport screening, walls and door locks, security expert Bruce Schneier has said.¹⁰⁹

There are a number of “insider” and “outsider” threats to the massive identification database connecting 56 States and territories. Creating a national identification database containing personal data of 245 million State license and ID cardholders nationwide, one that would be accessible from a massive number of DMVs across the country, is an invitation for all criminals – whether identity thieves or terrorists – to break into just one of these entrance points to gather such data for misuse.

Such a system would also be at risk of abuse from authorized users, such as DMV employees, who are bribed or threatened into changing the system data or issuing “authentic” national identification cards. It is appropriate to note here that, on the day that DHS released the final regulations for REAL ID, “A Maryland Motor Vehicle Administration employee [...] and four others were indicted [...] on charges that they made and sold fake State driver’s licenses and identification cards in exchange for money.”¹¹⁰

Identity theft is a large and growing problem. A Federal Trade Commission report estimated 8.3 million victims in 2005 (the last year for which numbers are available).¹¹¹ Serious cases of identity theft cost victims \$1,200 - \$2,500.¹¹² In 10 percent of new account frauds, victims incurred at least \$3,000 in out-of-pocket expenses.¹¹³ Domestic violence survivors are particularly vulnerable because their economic situation may be more precarious than average, and they may have greater need for unsullied credit as they attempt to create independent economic lives.

Large-scale data breaches have occurred in State DMVs across the country; if the databases are linked under REAL ID, these breaches will only grow in scale. The Oregon DMV lost half a million records in 2005.¹¹⁴ Also that year, in Georgia, a dishonest insider exposed 465,000 records.¹¹⁵ In 2006, a computer with the personal data of 16,000 individuals was stolen from a North Carolina DMV.¹¹⁶ The list goes on, and the personal information of individuals will be endangered under the REAL ID national identification system.

Domestic violence survivors are particularly vulnerable. Domestic violence survivors who flee their abusers, crossing into different States, would be exposed if their abuser breaches the security of any one of these 56 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.”¹¹⁷

Intentional breaches by outsiders or authorized insiders abusing their power would also have a wider scope under the Department of Homeland Security’s REAL ID national identification system. Past abuses exemplify what can be expected in a nationwide scale. For example, in September, a former Department of Commerce agent was indicted and charged with using a federal database to stalk a former girlfriend and her family.¹¹⁸ While employed at the Commerce Department, the agent is alleged to have accessed the system at least 163 times during a 10-month period.¹¹⁹ In Arizona, a police officer admitted accessing motor vehicle records to find personal information on women he was romantically interested in, as well as co-workers.¹²⁰

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 in 2007 – 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 man.¹²¹ This sort of inadvertence will happen much more frequently in a post-REAL ID world as the access to driver’s license information is spread throughout the national identification system.

C. Background Check Procedures Fail to Address Insider Threat Problems

The Department of Homeland Security requires certain government employees undergo criminal history background checks and list particular offenses that would disqualify an individual from specific jobs related to the REAL ID national identification system.¹²² In the draft regulations, DHS said employees who had to undergo these checks 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.¹²³ Employees who could access the record information without the ability to edit it are not subject to the background check requirement.

EPIC explained in our May 2007 comments, “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.”¹²⁴ We proposed that “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” in order to safeguard against these threats.¹²⁵ However, the final rule did not use this proposal.

In the draft regulations, the suitability criteria of the background check did not match the threat of stalkers and abusers. DHS proposed using 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. 1572.103.¹²⁶ The offenses include espionage, sedition, treason, making bomb threats, and crimes involving transportation security incidents.¹²⁷ 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.¹²⁸ However, crimes such as stalking, surveillance, harassment and domestic abuse are not in this list.

Recognizing the risk of improper access to the record system, EPIC recommended that, “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.”¹²⁹ The Department of Homeland Security

did not add these offenses, allowing even convicted abusers the opportunity to access to the massive national database created under REAL ID.¹³⁰

D. Final Rule Includes Marginal Improvements for Address Confidentiality and Name History Problems

Many States have created formal Address Confidentiality Programs and also provided general measures of residential address privacy, but these protections would be removed by the draft regulations.¹³¹ The final rule improves on some of the address confidentiality provisions of the proposed rule, but the subject of addresses in the national ID database is treated in contradictory manners in different parts of the final rule.

The REAL ID Act requires that driver's licenses include a person's "address of principle residence."¹³² This requirement effectively destroys State address confidentiality programs. The 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."¹³³ 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 from disclosure according to Section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act 1996.¹³⁴

In the final rule, the Department of Homeland Security includes more exemptions and extends them to the unencrypted machine-readable zone. Now exempt are individuals for whom State law, regulation, or DMV procedure permits display of an alternative address.¹³⁵ This exemption includes States that generally permit a mailing address to be displayed on the card. Individuals who are enrolled in address confidentiality programs, who have their information suppressed by court orders (including administrative orders), and those who are also protected by Section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 may also use an alternative address.¹³⁶ The unencrypted machine-readable zone requires the "address as listed on the card pursuant to § 37.17(f)" which includes the alternative address provisions.¹³⁷ Further, the final regulations require two documents that show "address of principle residence" but exempt street addresses pursuant to § 37.17(f), the section on that regulates address confidentiality.¹³⁸

The agency's comments to the final rule state, "true addresses must be captured and stored in a secure manner in the DMV database even if an alternate address appears on the face and MRZ portions of the driver's license or identification card."¹³⁹ However, the actual regulation that describes the design

of the national identification database, § 37.33, does not appear to incorporate these requirements. Under § 37.33 the database must contain:

- (1) All data fields printed on driver's licenses and identification cards issued by the State, individual serial numbers of the card, and SSN;
- (2) A record of the full legal name and recorded name established under Sec. 37.11(c)(2) as applicable, without truncation;
- (3) All additional data fields included in the MRZ but not printed on the driver's license or identification card; and
- (4) Motor vehicle driver's histories, including motor vehicle violations, suspensions, and points on driver's licenses.¹⁴⁰

The gathering, retention and distribution of addresses in the databases are unclear, as the Department of Homeland Security has made contradictory statements.

Though the treatment of name history is improved in the final rule, a significant problem remains. Name histories may be kept in motor vehicle databases and thus exposed to security breaches by insiders with access or outsiders who break into any one of the many DMVs across the country with access to the national database.

The final rule allows State law or regulation to permit the use of a name other than the one on the source documents.¹⁴¹ The State may itself determine what evidence is needed for it to accept the name if it differs from source documents.¹⁴² Further, the name difference from the source document must be recorded.¹⁴³ The final regulations also permit the name on the face of the card and in the machine-readable zone to deviate from the name on source documents.¹⁴⁴ These are all improvements over the draft regulations.

However, the final rule for implementation of the REAL ID system still contains a problematic name history provision. The DMV database is required to have "a record of the full legal name and recorded name established under §37.11(c)(2) as applicable, without truncation."¹⁴⁵ This record includes copies of source documents and any evidence of a name change.¹⁴⁶ Such data gathering, retention and distribution would leave a trail for abusers to follow.

IV. REAL ID SYSTEM CREATES NEW NATIONAL SECURITY RISKS

The Department of Homeland Security continues to claim that the national identification system created under the REAL ID scheme will improve national security. When releasing the final rule in January, Secretary Chertoff said, "secure identification is an essential way of ensuring that people are who they say they are. And therefore this kind of identification gives us a tremendous

tool in preventing dangerous people from getting on airplanes or getting into federal buildings.”¹⁴⁷ Yet there is a multitude of evidence that Secretary Chertoff is wrong – including evidence from the 9/11 Commission.

DHS’s national security rationale has always been confusing and has not changed since the draft regulations were released in March 2007. Our May 2007 comments included a detailed debunking of the Department of Homeland Security’s mystifying quantitative risk assessment.¹⁴⁸ The agency claimed this assessment proved the need for, cost-effectiveness of, and security advantages of the REAL ID national identification system.¹⁴⁹ Yet , DHS admitted at the time, “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.”¹⁵⁰ DHS attempted to determine the *marginal* chance that REAL ID will lessen the chance of success or discourage the attempt of a terrorist attack, using a number of faulty assumptions.

In the final regulations, the Department of Homeland Security again attempts a national security rationale, stating:

Under this final rule, it will be significantly more difficult for an individual to use a false name or provide fraudulent documents to obtain an identification that can be used for purposes of boarding a commercial airplane. Therefore, the final rule makes it less likely that a terrorist could circumvent watch-list screening processes and security procedures (as upgraded or developed post-9/11) and board a commercial airplane.¹⁵¹

However, in the final rule, the Department of Homeland Security includes an exception that completely undercuts the supposed security rationale for the creation of this national identification system. In the final rule, the Department of Homeland Security allows individuals to show their foreign passport in place of REAL ID card or other US-issued identification document.¹⁵² Criminals who do not wish to go through the cumbersome REAL ID process could merely go to any number of foreign countries and obtain (whether legally or illegally) a passport that would “prove” their identity as a “trusted” individual, one whose name is not on any watch lists.

All of the 9/11 hijackers could have boarded commercial flights or entered federal buildings under the REAL ID scheme because each hijacker had a foreign passport, according to the 9/11 Commission Report.¹⁵³ In fact, “potential hijackers [were told] to acquire new ‘clean’ passports in their home countries before applying for a U.S. visa. This was to avoid raising suspicion about previous travel to countries where al Qaeda operated,” said the Commission.¹⁵⁴ The 9/11 Commission in 2004 detailed the problem with the national security rationale that DHS continues to use in 2008.

Also, note that the Department of Homeland Security says in the final rule that it will be “significantly more difficult,” but not impossible, “for an individual to use a false name or provide fraudulent documents to obtain an identification.” This is the reason that any national identification system is fundamentally flawed: Individuals are told to “trust” the national ID card, but it is still possible to create a fake card, so one cannot rely on the national identification system to “prove” an individual is who she says. Contrary to the Department of Homeland Security’s claims, this system harms our national security by creating another “trusted” path for criminals to exploit.

V. STATES OPPOSE NATIONAL ID SYSTEM

Since the passage of the REAL ID Act in 2005, a number of States have passed legislation rejecting the national identification system. On January 18, Montana governor Brian Schweitzer wrote to the governors of 17 States asking them to join him in rejecting the REAL ID system.¹⁵⁵ “Today, I am asking you to join with me in resisting the DHS coercion to comply with the provisions of REAL ID,” Gov. Schweitzer wrote. “I would like us to speak with one, unified voice and demand the Congress step in and fix this mess.”¹⁵⁶

Four states (Maine, Montana, New Hampshire and South Carolina) have expressly rejected the system and none asked for an extension. After much posturing, DHS gave extensions to all States, even though some said they would never implement REAL ID, because their legislatures have passed laws banning the national identification system.¹⁵⁷

In the final regulations released in January, the Department of Homeland Security set an extension request deadline of March 31, 2008.¹⁵⁸ By that date, all 56 States and U.S. territories were required to ask the agency for an extension that would allow their licenses and ID cards to remain “valid for federal purposes” past May 11, 2008 through the first extension period, until December 31, 2009.¹⁵⁹ For States that do ask for the initial extension, those States then have until October 11, 2009 to “file a request for an additional extension until no later than May 10, 2011, by submitting a Material Compliance Checklist demonstrating material compliance.”¹⁶⁰

The extensions were necessary because, even though May 11, 2008 is the statutory deadline for implementation of the REAL ID system, not one State is in compliance with the federal law creating a national identification system. In fact, 19 States have passed resolutions or laws rejecting the national ID program.

The Department of Homeland Security said it “made extensions available for states that needed additional time to come into compliance, or to complete

ongoing security measures,” implying that states that received extensions had agreed to implement the REAL ID national identification system.¹⁶¹ However, a number of states have said that these extensions do not constitute an agreement to implement this national ID scheme.

For example, California (one of the most populous states) sent a letter to the Department of Homeland Security on March 18, stating, “California’s request for an extension is not a commitment to implement REAL ID.”¹⁶² New Hampshire said, “because our Legislature voted overwhelmingly in 2007 to pass a bill that prohibits our state from implementing the REAL ID Act in New Hampshire, we cannot authorize implementation of the REAL ID regulations.”¹⁶³

There are also ongoing concerns about Homeland Security’s cost computation. In the final regulations, DHS claims to reduce the cost of implementation for the REAL ID national identification system to \$9.9 billion, a significant drop from the draft regulations’ estimate of \$23.1 billion.¹⁶⁴ However, there are significant problems with the agency’s assumptions.

The agency assumes that only 75 percent of U.S. residents will not apply for a REAL ID national identification card.¹⁶⁵ DHS states that the remaining 25 percent will either not enter federal buildings or board commercial flights, or the people will use \$100 U.S. passports.¹⁶⁶ The agency also ignores, among other things, the cost of creating the national identification database (or “hub” network) linking 56 States and territories.

The Department of Homeland Security also believes that it can sweep aside the fact that REAL ID is an unfunded mandate by allocating \$360 million to the States for REAL ID implementation. The agency said it will offer, “\$80 million in dedicated REAL ID grants and another \$280 million in general funding as part of the Homeland Security Grant Program,” which funds security programs such as first responder services.¹⁶⁷ However, the number still pales next to the agency’s “reduced” estimate of \$9.9 billion.

Currently Congress is considering legislation to repeal REAL ID.¹⁶⁸ Sen. Patrick Leahy, who co-sponsored legislation to replace REAL ID with the negotiated rulemaking process originally enacted in the 2004 Intelligence Reform and Terrorist Prevention Act, criticized the final regulations. “The Bush administration’s REAL ID program will not only lead to long lines at every DMV across the country, it will impose a massive unfunded mandate on State governments while offering absolutely no federal privacy protections to our citizens,” Sen. Leahy said.¹⁶⁹ “It is unfortunate that instead of addressing the fundamental problems this law poses for the States, the Administration appears content merely to prolong a contentious and unproductive battle to force the States to comply.”

VI. RECOMMENDATION: DECENTRALIZE IDENTIFICATION

The REAL ID national identification system would harm rather than protect privacy and security, and such a system would exacerbate the country's growing identity theft problem. 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.¹⁷⁰

A system of decentralized identification reduces the risks associated with security breaches and the misuse of personal information. Technological innovation can enable the development of context-dependent identifiers. A decentralized approach to identification is consistent with our commonsense understanding of identification. If you are banking, you should have a bank account number. If go to the library, you should have a library card number. If you rent videos from a store, you should have a video rental store card number. Utility bills, telephone bills, insurance, the list goes on. These context-dependent usernames and passwords enable authentication without the risk of a universal identification system. That way, if one number is compromised, all of the numbers are not spoiled and identity thieves cannot access all of your accounts. All of your accounts can become compartmentalized, enhancing their security.¹⁷¹

Internet companies are already moving to develop systems of multiple identification in part because of concerns that were identified in a consumer privacy case brought to the Federal Trade Commission ("FTC") in 2001. In that matter, EPIC and 12 organizations submitted a complaint to the FTC, detailing serious privacy implications of Microsoft Windows XP and Microsoft Passport.¹⁷² The complaint alleged that Microsoft "has engaged, and is engaging, in unfair and deceptive trade practices intended to profile, track, and monitor millions of Internet users," and that the company's collection and use of personal information violated Section 5 of the Federal Trade Commission Act.¹⁷³

In August 2002, the FTC announced a settlement in its privacy enforcement action against Microsoft.¹⁷⁴ The settlement required that Microsoft establish a comprehensive information security program for Passport, and prohibited any misrepresentation of its practices regarding information collection and usage.

Since the FTC settlement of the EPIC complaint against Passport, industry groups have moved toward decentralized identity systems that are more robust, provide more security, and are better for privacy. Microsoft has developed an approach to identity management that allowed for multiple forms of online identification, and other companies, including open source developers, followed a similar approach.¹⁷⁵ There is a need to avoid single identifiers and to promote

multiple identification schemes, and that this approach is best not only for privacy but also for security.

The development of system for multiple identification, or “meta-identification” is widely favored by experts in the field. For example, Jim Harper, Director of Information Policy Studies at the Cato Institute, explains that the REAL ID Act does not add to the nation’s security protections.¹⁷⁶ Instead, Harper advocates a diverse identification system. “A diverse, competitive identification and credentialing industry would be far better, and far more protective of liberty, than the uniform government-monopolized identification system on the advance today.”¹⁷⁷

VII. CONCLUSION

When Congress created the Department of Homeland Security, it made clear in the enabling legislation that the agency could not create a national ID system.¹⁷⁸ 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.”¹⁷⁹

In an opinion column written by Secretary Chertoff after the publication of the final rule, he said, “embracing REAL ID” would mean it would be used to “cash a check, hire a baby sitter, board a plane or engage in countless other activities.”¹⁸⁰ This is a description of a national identification system, which is illegal in the United States.

The final rule includes few protections for individual privacy and security in its massive national identification database. It harms national security by creating yet another “trusted” credential for criminals to exploit. The Department of Homeland Security has faced so many obstacles with the REAL ID system that the agency now plans an implementation deadline of 2017 – nine years later than the 2008 statutory deadline.¹⁸¹ It is an unfunded mandate that would cost billions, with the burden ultimately being placed on the individual taxpayer.

Technical experts familiar with the challenges of privacy protection and identification presented the Department of Homeland Security with a variety of recommendations that would have minimized the risks of the REAL ID system. The DHS made some modifications, but left the essential system in place. As REAL ID currently stands, the costs are many and the benefits are few. Public opposition to implementation is understandable.

Appendix I

STATE LEGISLATION AGAINST REAL ID ACT

State Legislation Against REAL ID Act	
Alaska, SB 202 (April 11, 2008)*	Colorado, HJR 1047 (May 14, 2007)
South Dakota, SCR 7 (February 25, 2008)	Georgia, SB 5 (May 11, 2007)
Tennessee, SJR 0248 (June 14, 2007)	Hawaii, SCJ 31 (April 25, 2007)
South Carolina, S 449 (June 5, 2007)	North Dakota, SCR 4040 (April 20, 2007)
Nebraska, LR 28 (May 30, 2007)	Washington SB 5087 (April 18, 2007)
New Hampshire, HB 685 (May 24, 2007)	Montana, HB 287 (April 17, 2007)
Oklahoma, SB 464 (May 23, 2007)	Arkansas, SCR 22 (March 28, 2007)
Illinois, HJR 0027 (May 22, 2007)	Idaho: HJM 3 (March 12, 2007) HB 606 (April 9, 2008)
Missouri, HCR 20 (May 17, 2007)	Maine, SP 113 (January 25, 2007)
Nevada, AJR 6 (May 14, 2007)	
<i>*Date passed</i>	Source: http://epic.org/privacy/id-cards/

Appendix II

EPIC EXPERT COMMENTS ON DRAFT REAL ID REGULATIONS

“EPIC and 24 Experts in Privacy and Technology, Comments on DHS 2006-0030: Notice of Proposed Rulemaking: Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes (May 8, 2007),” available at http://www.epic.org/privacy/id_cards/epic_realid_comments.pdf.

Signatories (affiliations are for identification only)

Steven Aftergood, Director of Project on Government Secrecy, Federation of American Scientists

Anita Allen, J.D., Ph.D., Henry R. Silverman Professor of Law and Professor of Philosophy, University of Pennsylvania Law School

Ann Bartow, Associate Professor of Law, University of South Carolina School of Law

Christine L. Borgman, Professor & Presidential Chair in Information Studies, University of California, Los Angeles

James Boyle, William Neal Reynolds Professor of Law, Duke University School of Law

David Chaum, Founder, DigiCash Inc.

Julie E. Cohen, Professor of Law, Georgetown University Law Center

Simon Davies, Director General, Privacy International

Dr. Whitfield Diffie, Chief Security Officer, Sun Microsystems

David Farber, Distinguished Career Professor of Computer Science and Public Policy, Carnegie Mellon University

Philip Friedman, Friedman Law Offices, PLLC

Deborah Hurley, Chair, EPIC Board of Advisors

Jerry Kang, Professor of Law, UCLA School of Law

Chris Larsen, CEO, Prosper Marketplace, Inc.

Gary Marx, Professor Emeritus, Massachusetts Institute of Technology

Mary Minow, LibraryLaw.com

Dr. Peter G. Neumann, Principal Scientist, SRI International Computer Science Lab

Dr. Deborah Peel, Founder, Patients Privacy Rights

Stephanie Perrin, Director of Integrity Policy, Service Canada

Anita Ramasastry, Associate Professor of Law, University of Washington School of Law

Dr. Bruce Schneier, Chief Technical Officer, BT Counterpane

Robert Ellis Smith, Publisher, Privacy Journal

Daniel J. Solove, Associate Professor of Law, George Washington
University Law School

Frank M. Tuerkheimer, Professor of Law Emeritus, University of
Wisconsin Law School

End Notes

-
- ¹ See generally, EPIC, National ID Cards and the REAL ID Act, http://www.epic.org/privacy/id_cards/.
- ² See EPIC AND PRIVACY INTERNATIONAL, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND PRACTICE 23-41 (EPIC 2006).
- ³ *Id.* at 23-24.
- ⁴ Dep't of Health, Educ. & Welfare, Secretary's Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* 125-35 (MIT 1973) [hereinafter "HEW Report on Data Systems"], available at <http://www.epic.org/privacy/hew1973report/>.
- ⁵ See generally, EPIC, Social Security Numbers, <http://www.epic.org/privacy/ssn/>.
- ⁶ Soc. Sec. Admin., Soc. Sec. Number Task Force, *Report to the Commissioner* (May 1971).
- ⁷ HEW Report on Data Systems at 125-35 (MIT 1973), *supra* note 4.
- ⁸ Dep't of Justice, Fed. Advisory Comm. on False Identification, *The Criminal Use of False Identification* (Nov. 1976).
- ⁹ Privacy Prot. Study Comm'n, *Personal Privacy in an Information Society* (July 1977) available at <http://www.epic.org/privacy/ppsc1977report/>.
- ¹⁰ *Id.*
- ¹¹ Robert B. Cullen, *Administration Announcing Plan*, ASSOCIATED PRESS, July 30, 1981.
- ¹² Press Release, White House Office of the Press Secretary, The Health Security Act Of 1993: Health Care That's Always There (Sept. 22, 1993) available at <http://www.clintonfoundation.org/legacy/092293-press-release-on-health-security-plan.htm>.
- ¹³ Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, Div. C, Title III, § 309 (1996), amended by the Immigration and Naturalization Service Data Management Improvement Act of 2000, Pub. L. No. 106-215, 114 Stat. 337 (2000).
- ¹⁴ Summer Lemon, *Ellison offers free software for national ID card*, IDG.NET, Sept. 25, 2001, available at <http://archives.cnn.com/2001/TECH/industry/09/25/ellison.software.idg/>.
- ¹⁵ Declan McCullagh, *Oracle Keeps Pushing ID Card*, WIRED NEWS, Nov. 17, 2001, available at <http://www.wired.com/news/politics/0,1283,48482,00.html>.
- ¹⁶ Homeland Security Act of 2002 § 554, 6 U.S.C. § 554 (2004).
- ¹⁷ *Id.*
- ¹⁸ Such proposals include the Western Hemisphere Travel Initiative PASSCard and "enhanced" driver's licenses with citizenship designations. See EPIC, *Comments on Docket No. USCBP-2007-0061: Proposed Rule: Documents Required for Travelers Departing From or Arriving in the United States From Within the Western Hemisphere* (Aug. 1, 2007), available at http://www.epic.org/privacy/rfid/whti_080107.pdf; EPIC, *Spotlight on Surveillance, Proposed 'Enhanced' Licenses Are Costly to Security and Privacy*, <http://epic.org/privacy/surveillance/spotlight/0907/>.
- ¹⁹ Pub. L. No. 109-13, 119 Stat. 231 (2005) [hereinafter "REAL ID Act"].
- ²⁰ 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://hsgac.senate.gov/public/index.cfm?FuseAction=PressReleases.Detail&Affiliation=C&PressRelease_id=b456811f-b97a-4d4c-8503-cacbaaa649ca&Month=4&Year=2005.
- ²¹ *Id.*
- ²² EPIC, "National ID at the Crossroads: The Future of Privacy in America," (June 6, 2005) (a public conference on "The technology of identification; Lessons of RFID passports; and An organized response to REAL ID"), <http://epic.org/events/id/>.
- ²³ 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) [hereinafter "REAL ID Draft Regulations"], available at <http://edocket.access.gpo.gov/2007/07-1009.htm>; see generally, 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>.

²⁴ EPIC and 24 Experts in Privacy and Technology, *Comments on DHS 2006-0030: Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes* (May 8, 2007) [hereinafter "EPIC Expert Comments on Draft Regulations"], available at http://www.epic.org/privacy/id_cards/epic_realid_comments.pdf. See Appendix II.

²⁵ Privacy Coalition, "Speak Out Against REAL ID," <http://privacycoalition.org/stoprealid/>.

²⁶ Though the Department of Homeland Security announced the final rule on Jan. 11, 2008, it was not published in the Federal Register until 18 days later. Dep't of Homeland Sec., *Final Rule, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, 73 Fed. Reg. 5271 (Jan. 29, 2008) [hereinafter "REAL Final Rule"], available at <http://edocket.access.gpo.gov/2008/08-140.htm>.

²⁷ See discussion in Section IX. *Recent Developments: States Continue Rebellion Against National ID System*.

²⁸ *Id.*; Also, 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* *supra* note 20.

²⁹ See ACLU, *Real Nightmare: What's Wrong with REAL ID*, <http://realnightmare.org/>; and Identity Project, <http://www.papersplease.org/wp/>.

³⁰ Security expert Bruce Schneier has detailed a number of problems with REAL ID in publications and Congressional testimony. See CRYPTO-GRAM newsletter, <http://www.schneier.com/crypto-gram-back.html>.

³¹ Michael Chertoff, Sec'y, Dep't of Homeland Security, *Remarks at a Press Conference on REAL ID*, Jan. 11, 2008 [hereinafter "Chertoff Remarks on Final Rule"], available at http://www.dhs.gov/xnews/speeches/sp_1200320940276.shtm.

³² *Id.*

³³ *Id.*

³⁴ *Id.*

³⁵ 5 U.S.C. § 552a (1974).

³⁶ EPIC Expert Comments on Draft Regulations at 3, *supra* note 24.

³⁷ *Id.* at 4, quoting Richard C. Barth, Assistant Sec'y for Policy Dev., 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), available at http://hsgac.senate.gov/public/_files/Testimonybarth.pdf.

³⁸ See e.g., Comm'n on Fed. Election Reform (aka "Carter-Baker Commission"), *Building Confidence in U.S. Elections* (Sept. 2005), available at http://www.american.edu/ia/cfer/report/full_report.pdf.

³⁹ REAL Final Rule at 5288, *supra* note 26.

⁴⁰ *Id.* at 5319. In March 2007, a Homeland Security official testified to Congress that "widespread acceptance" of REAL ID would affect employment and voting. See Richard C. Barth, *supra* note 37.

⁴¹ Chertoff Remarks on Final Rule, *supra* note 31.

⁴² REAL Final Rule at 5329, *supra* note 26.

⁴³ Ryan Singel, *Montana Governor Foments Real ID Rebellion*, WIRED, Jan. 18, 2008, <http://blog.wired.com/27bstroke6/2008/01/montana-governo.html>.

⁴⁴ *Id.*

- ⁴⁵ Dep't of State, Passport Fees, http://travel.State.gov/passport/get/fees/fees_837.html.
- ⁴⁶ REAL Final Rule at 5322, *supra* note 26.
- ⁴⁷ REAL ID Act at §§ 202(c)(1), 202(c)(2)(B), *supra* note 19.
- ⁴⁸ REAL Final Rule at 5333, *supra* note 26.
- ⁴⁹ *Id.* at 5277.
- ⁵⁰ EPIC Expert Comments on Draft Regulations at 13, *supra* note 24.
- ⁵¹ *Id.* at 14.
- ⁵² *Id.* at 53-54.
- ⁵³ REAL Final Rule at 5334, *supra* note 26.
- ⁵⁴ *Id.* at 5298.
- ⁵⁵ *Id.* at 5334.
- ⁵⁶ REAL ID Draft Regulations at 10,822, *supra* note 23.
- ⁵⁷ REAL Final Rule at 5315, *supra* note 26.
- ⁵⁸ *Id.* at 5298.
- ⁵⁹ EPIC Expert Comments on Draft Regulations at 14-17, *supra* note 24.
- ⁶⁰ REAL Final Rule at 5296, 5334, *supra* note 26; Electronic Verification of Vital Events ("EVVE") is also called Electronic Verification of Vital Event Records ("EVVER") in some federal documents.
- ⁶¹ Nat'l Governors Ass'n, et. al, *The REAL ID Act: National Impact Analysis* (Sept. 19, 2006), available at <http://www.nga.org/Files/pdf/0609REALID.PDF>.
- ⁶² See EPIC, Social Security Numbers, *supra* note 5 and EPIC, Spotlight on Surveillance, *Proposed 'Enhanced' Licenses Are Costly to Security and Privacy*, <http://epic.org/privacy/surveillance/spotlight/0907/>.
- ⁶³ Office of Inspector Gen., Soc. Sec. Admin, *Congressional Response Report: Accuracy of the Social Security Administration's Numident File, A-08-06-26100 6* (Dec. 18, 2006), available at <http://www.ssa.gov/oig/ADOBEPDF/A-08-06-26100.pdf>.
- ⁶⁴ *Id.* at Appendix C-2.
- ⁶⁵ Office of Inspector Gen., Dep't of Justice, *Immigration and Naturalization Service Monitoring of Nonimmigrant Overstays, Rept. No. I-97-08* (Sept. 1997), available at <http://www.usdoj.gov/oig/reports/INS/e9708/index.htm>; *Follow-Up Report on INS Efforts to Improve the Control of Nonimmigrant Overstays, Rept. No. I-2002-006* (Apr. 2002), available at <http://www.usdoj.gov/oig/reports/INS/e0206/index.htm>; and *Immigration and Naturalization Service's Ability to Provide Timely and Accurate Alien Information to the Social Security Administration, Rept. No. I-2003-001* (Nov. 2002), available at <http://www.usdoj.gov/oig/reports/INS/e0301/final.pdf>.
- ⁶⁶ *AFL-CIO v. Chertoff*, No. C 07-04472 CRB (N.D. Cal. 2007), available at http://www.aclu.org/images/asset_upload_file505_32133.pdf.
- ⁶⁷ REAL Final Rule at 5297, *supra* note 26.
- ⁶⁸ EPIC Expert Comments on Draft Regulations at 15-16, *supra* note 24, citing REAL ID Draft Regulations at 10,833, *supra* note 23.
- ⁶⁹ REAL Final Rule at 5275-5276, *supra* note 26.
- ⁷⁰ *Id.* at 5297.
- ⁷¹ "As of October 2007 [the most recent data available], the following vital records offices are online with EVVE: Arkansas, Hawaii, Iowa, Kentucky, Minnesota, Mississippi, Missouri, Montana, North Dakota, South Dakota and Utah." Nat'l Ass'n for Public Health Statistics & Info. Systems, *Electronic Verification of Vital Events (EVVE)*, <http://www.naphsis.org/index.asp?bid=1036>.
- ⁷² REAL ID Draft Regulations at 10,831, *supra* note 23.
- ⁷³ REAL Final Rule at 5297, *supra* note 26.
- ⁷⁴ REAL ID Draft Regulations at 10,832, *supra* note 23.
- ⁷⁵ REAL Final Rule at 5297, *supra* note 26.
- ⁷⁶ *Id.*
- ⁷⁷ EPIC Expert Comments on Draft Regulations at 16-17, *supra* note 24.

⁷⁸ REAL Final Rule at 5277, *supra* note 26.

⁷⁹ REAL Final Rule at 5333, *supra* note 26.

⁸⁰ *Id.* at 5277.

⁸¹ 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 122 (Feb. 28, 2007) [hereinafter "DHS's Regulatory Evaluation of Draft REAL ID Regulations"], available at http://www.epic.org/privacy/id_cards/reg_eval_draftregs.pdf.

⁸² REAL Final Rule at 5338, *supra* note 26.

⁸³ 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>.

⁸⁴ *Id.* at 19.

⁸⁵ EPIC Expert Comments on Draft Regulations at 17, *supra* note 24.

⁸⁶ REAL ID Draft Regulations at 10,825, *supra* note 23.

⁸⁷ Sen. Joseph Lieberman, *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).

⁸⁸ EPIC Expert Comments on Draft Regulations at 6-12, *supra* note 24.

⁸⁹ Office of Mgmt. & Budget, *Privacy Act Implementation: Guidelines and Responsibilities*, 40 Fed. Reg. 28,948, 28,951 (July 9, 1975), available at http://www.whitehouse.gov/omb/inforeg/implementation_guidelines.pdf.

⁹⁰ *Id.*

⁹¹ 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.

⁹² *Id.* at 1.

⁹³ REAL Final Rule at 5284-5284, *supra* note 26.

⁹⁴ EPIC Expert Comments on Draft Regulations at 17-28, *supra* note 24.

⁹⁵ REAL ID Act at § 202(b), *supra* note 19.

⁹⁶ REAL Final Rule at 5336, *supra* note 26.

⁹⁷ Dep't of Homeland Sec., Data Privacy & Integrity Advisory Committee, "The Use of RFID for Human Identity Verification," Report No. 2006-02 (Adopted Dec. 6, 2006), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf. See also, Wilson Dizard, *DHS privacy office slams RFID technology*, COMPUTERWORLD, May 7, 2006, available at http://www.gcn.com/online/vol1_no1/40808-1.html.

⁹⁸ *Id.* at 5292.

⁹⁹ Dep't of Homeland Sec. Privacy Office, *Privacy Impact Assessment for the REAL ID Act* 16 (Mar. 1, 2007), available at http://www.epic.org/privacy/id_cards/pia_030107.pdf.

¹⁰⁰ EPIC Expert Comments on Draft Regulations at 21-23, *supra* note 24.

¹⁰¹ *Id.*

¹⁰² *Id.* at 17-18.

¹⁰³ REAL Final Rule at 5292, *supra* note 26.

¹⁰⁴ EPIC Expert Comments on Draft Regulations at 19, *supra* note 24.

¹⁰⁵ REAL ID Act at § 202(b)(8), *supra* note 19.

¹⁰⁶ REAL Final Rule at 5275, 5291, *supra* note 26.

¹⁰⁷ EPIC Expert Comments on Draft Regulations at 31-33, *supra* note 24.

¹⁰⁸ 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.* (Mar. 21, 2007), available at http://www.epic.org/privacy/id_cards/ngo_test_032107.pdf.

-
- ¹⁰⁹ Press Release, EPIC, *After Long Delay, Homeland Security Department Announces Regulations For Deeply Flawed National ID System* (Jan. 11, 2008), *available at* <http://epic.org/press/011108.html>.
- ¹¹⁰ *Five indicted in identity theft scheme*, BALTIMORE SUN, Jan. 11, 2008.
- ¹¹¹ Fed. Trade Comm'n, *2006 Identity Theft Survey Report 3* (Nov. 2007), *available at* <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>.
- ¹¹² *Id.* at 5.
- ¹¹³ *Id.* at 6.
- ¹¹⁴ Privacy Rights Clearinghouse, *A Chronology of Data Breaches*, <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.
- ¹¹⁵ *Id.*
- ¹¹⁶ *Id.*
- ¹¹⁷ EPIC Expert Comments on Draft Regulations at 50, *supra* note 24.
- ¹¹⁸ Press Release, Dep't of Justice, *Former Department of Commerce Agent Indicted For Making a False Statement and Exceeding Authorized Access To a Government Database* (Sept. 19, 2007), *available at* http://www.usdoj.gov/usao/can/press/2007/2007_09_19_robinson.indicted.press.html.
- ¹¹⁹ *Id.*
- ¹²⁰ Michael Kiefer, *Officer Admits to Tampering; Databases Used to Check on Women*, ARIZONA REPUBLIC, April 6, 2006, at 3B. More insider and outsider abuses are detailed in our May 2007 comments. EPIC Expert Comments on Draft Regulations at 45, 50-51, *supra* note 24.
- ¹²¹ Kevin Murphy, *Officer's Actions will Cost 25,000*, GAZETTEEXTRA, Feb. 15, 2007, <http://www.gazetteextra.com/mezera021507.asp>.
- ¹²² REAL Final Rule at 5338, *supra* note 26.
- ¹²³ REAL ID Draft Regulations at 10,856, *supra* note 23.
- ¹²⁴ EPIC Expert Comments on Draft Regulations at 51, *supra* note 24.
- ¹²⁵ *Id.*
- ¹²⁶ REAL ID Draft Regulations at 10,856, *supra* note 23.
- ¹²⁷ 49 C.F.R. 1572.103(a).
- ¹²⁸ *Id.* at 1572.103(b)(2)(iii).
- ¹²⁹ EPIC Expert Comments on Draft Regulations at 52, *supra* note 24.
- ¹³⁰ REAL Final Rule at 5338, *supra* note 26.
- ¹³¹ EPIC Expert Comments on Draft Regulations at 46-50, *supra* note 24.
- ¹³² REAL ID Act at § 202(b)(6), *supra* note 19.
- ¹³³ Violence Against Women & Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, § 827, 119 Stat. 2960, 3066 (2005) [hereinafter "VAWA"].
- ¹³⁴ *Id.*
- ¹³⁵ REAL Final Rule at 5335, *supra* note 26.
- ¹³⁶ *Id.*
- ¹³⁷ *Id.* at 5336.
- ¹³⁸ *Id.* at 5333.
- ¹³⁹ *Id.* at 5302.
- ¹⁴⁰ REAL Final Rule at 5337, *supra* note 26.
- ¹⁴¹ *Id.* at 5300.
- ¹⁴² *Id.* at 5333.
- ¹⁴³ *Id.*
- ¹⁴⁴ *Id.* at 5335-36.
- ¹⁴⁵ REAL Final Rule at 5337, *supra* note 26.
- ¹⁴⁶ *Id.*
- ¹⁴⁷ Chertoff Remarks on Final Rule, *supra* note 31.
- ¹⁴⁸ EPIC Expert Comments on Draft Regulations at 33-39, *supra* note 24.
- ¹⁴⁹ *Id.*

-
- ¹⁵⁰ DHS's Regulatory Evaluation of Draft REAL ID Regulations at 127, *supra* note 81.
- ¹⁵¹ REAL Final Rule at 5285, *supra* note 26.
- ¹⁵² *Id.* at 5333.
- ¹⁵³ Nat'l Comm'n on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (July 2004), available at <http://govinfo.library.unt.edu/911/report/index.htm>.
- ¹⁵⁴ *Id.* at 236.
- ¹⁵⁵ Letter from Montana Governor Brian Schweitzer to 17 States (Jan. 18, 2008), available at http://governor.mt.gov/brian/RealID_080118.pdf.
- ¹⁵⁶ *Id.*
- ¹⁵⁷ Press Release, Dep't of Homeland Sec., All Jurisdictions Meet Initial REAL ID Requirements (Apr. 2, 2008), available at http://www.dhs.gov/xnews/releases/pr_1207167055742.shtm.
- ¹⁵⁸ REAL Final Rule at 5339, *supra* note 26.
- ¹⁵⁹ *Id.*
- ¹⁶⁰ *Id.*
- ¹⁶¹ Press Release, Dep't of Homeland Sec., Most Jurisdictions Meet Initial REAL ID Requirements (Apr. 1, 2008), available at http://www.dhs.gov/xnews/releases/pr_1207079095443.shtm.
- ¹⁶² Letter from George Valverde, Dir., Calif. Dep't of Motor Vehicles, to Michael Chertoff, Sec'y, Dep't of Homeland Sec., Mar. 18, 2008, available at http://epic.org/privacy/id-cards/calif_dhs_031808.pdf.
- ¹⁶³ Letter from Earl M. Sweeney, Assistant Comm'r, N.H. Dep't of Safety, to Stewart Baker, Assistant Sec'y for Policy, Dep't of Homeland Sec. Mar. 26, 2008, available at http://epic.org/privacy/id-cards/nj_dhs_032608.pdf.
- ¹⁶⁴ REAL Final Rule at 5324, *supra* note 26; EPIC Expert Comments on Draft Regulations at 33-39, 41-46, *supra* note 24.
- ¹⁶⁵ REAL Final Rule at 5322, *supra* note 26.
- ¹⁶⁶ *Id.*
- ¹⁶⁷ Press Release, Dep't of Homeland Sec., DHS Releases REAL ID Regulation, Jan. 11, 2008, available at http://www.dhs.gov/xnews/releases/pr_1200065427422.shtm.
- ¹⁶⁸ S. 717, *A bill to repeal title II of the REAL ID Act of 2005, to restore section 7212 of the Intelligence Reform and Terrorism Prevention Act of 2004, which provides States additional regulatory flexibility and funding authorization to more rapidly produce tamper- and counterfeit-resistant driver's licenses, and to protect privacy and civil liberties by providing interested stakeholders on a negotiated rulemaking with guidance to achieve improved 21st century licenses to improve national security*, 110th Cong. (2008); H.R. 1117, *A bill to repeal title II of the REAL ID Act of 2005, to reinstitute section 7212 of the Intelligence Reform and Terrorism Prevention Act of 2004, which provides States additional regulatory flexibility and funding authorization to more rapidly produce tamper- and counterfeit-resistant driver's licenses and to protect privacy and civil liberties by providing interested stakeholders on a negotiated rulemaking with guidance to achieve improved 21st century licenses to improve national security*, 110th Cong. (2008).
- ¹⁶⁹ Press Release, Office of Sen. Patrick Leahy, Reaction of Sen. Patrick Leahy (D-Vt.) on Release of the Final REAL ID Regulations by the U.S. Department of Homeland Security (Jan. 11, 2008), available at <http://leahy.senate.gov/press/200801/011108a.html>.
- ¹⁷⁰ For more discussion of identifiers, see EPIC, *Comments to the Federal Trade Commission on Private Sector Use of Social Security Numbers: Topics For Comment* (Sept. 5, 2007), available at http://www.epic.org/privacy/ssn/ftc_ssn_090507.pdf.
- ¹⁷¹ *Id.*
- ¹⁷² In the Matter of Microsoft Corporation File No. 012 3240, Docket No. C-4069 (Aug. 2002), available at <http://www.ftc.gov/os/caselist/0123240/0123240.shtm>.
- ¹⁷³ *Id.* at 1.
- ¹⁷⁴ Fed. Trade Comm'n, *Microsoft Settles FTC Charges Alleging False Security and Privacy Promises* (Aug. 2002) ("The proposed consent order prohibits any misrepresentation of information practices in connection with Passport and other similar services. It also requires Microsoft to

implement and maintain a comprehensive information security program. In addition, Microsoft must have its security program certified as meeting or exceeding the standards in the consent order by an independent professional every two years.”), *available at* <http://www.ftc.gov/opa/2002/08/microsoft.shtm>.

¹⁷⁵ Kim Cameron, *The Laws of Identity*, IDENTITY WEBLOG, Dec. 9, 2004, <http://www.identityblog.com/stories/2004/12/09/thelaws.html>; Windows CardSpace, <http://cardspace.netfx3.com/>; OpenCard, <http://www.opencard.org/>.

¹⁷⁶ JIM HARPER, IDENTITY CRISIS: HOW IDENTIFICATION IS OVERUSED AND MISUNDERSTOOD (Cato Institute 2006).

¹⁷⁷ *Id.* at 5.

¹⁷⁸ Pub. L. No. 107-296, 116 Stat. 2135 (2002).

¹⁷⁹ 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.

¹⁸⁰ Michael Chertoff, *National ID security*, SACRAMENTO BEE, Jan. 16, 2008, *available at* <http://www.sacbee.com/110/story/636479.html>.

¹⁸¹ REAL Final Rule at 5333, *supra* note 26.