Testimony of

Jim Harper

May 8, 2007

Testimony of Jim Harper, Director of Information Policy Studies
The Cato Institute
to the Senate Committee on the Judiciary
Will REAL ID Actually Make Us Safer? An Examination of Privacy and Civil Liberties Concerns

May 8, 2007
Chairman Leahy, Ranking Member Specter, and Members of the Committee:

It is a pleasure to speak with you today. I am director of information policy studies at the Cato Institute, a non-profit research foundation dedicated to preserving the traditional American principles of limited government, individual liberty, free markets, and peace. In that role, I study the unique problems in adapting law and policy to the information age. I also serve as a member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee, which advises the DHS Privacy Office and the Secretary of Homeland Security on privacy issues.

My most recent book is entitled Identity Crisis: How Identification Is Overused and Misunderstood. I am also editor of Privacilla.org, a Web-based think tank devoted exclusively to privacy, and I maintain an online resource about federal legislation and spending called WashingtonWatch.com. I speak only for myself today and not for any of the organizations with which I am affiliated or for any colleague.

* * * *

Mr. Chairman, the REAL ID Act is a dead letter. All that remains is for Congress to declare it so. The proposed regulations issued by the Department of Homeland Security on March 9th, on which comments close today, help reveal that REAL ID is a loser. It costs more to implement than it would add to our country's protections.

The regulations "punted" on REAL ID's most important technology, security, and privacy problems. Of utmost importance, the DHS proposal lays the groundwork for systematic tracking of Americans based on their race .
Though the Department of Homeland Security failed to "fix it in the regs," this is not the agency's fault. Regulations cannot make this law work, and neither can delay. The real problem is the REAL ID law itself.

There are highly meritorious bills pending in the Senate and House to repeal the REAL ID Act and restore the identification security provisions that were passed in the 9/11-Commission-inspired Intelligence Reform and Terrorism Prevention Act. Congratulations, Mr. Chairman for being an original cosponsor of this legislation in the Senate.

These bills would be improved if they were to chart a path to government use of emerging digital identity and credentialing systems that are diverse, competitive, and privacy protective. We can have identification and credentialing systems that maximize security and minimize surveillance. REAL ID is the ugly alternative to getting it right.

REAL ID Does Not Secure the Country

I will begin with security issues, which are the most important. Simply put, the proponents of REAL ID have not borne their burden of proof. They have not shown that REAL ID would add to our country's protections -- because it doesn't.

The Department of Homeland Security has had two years to articulate how REAL ID would work. But the cost-benefit analysis provided in the proposed rules issued in March (the notice of proposed rulemaking or "NPRM") helps show that implementing REAL ID would impose more costs on our society than it would provide security or other benefits. REAL ID would do more harm than good.

Executive Order 128661 requires agencies to assess the costs and benefits of the requirements they propose. In its cost-benefit analysis, the Department found that implementing REAL ID would cost over $17 billion.2 This is 50% higher than the $11 billion estimate put forward by the National Conference of State Legislators.3

The NPRM was the Department's opportunity to show how REAL ID might add to our country's protections. But on the question of benefits, the Department of Homeland Security essentially punted. It said:

It is impossible to quantify or monetize the benefits of REAL ID using standard economic accounting techniques. However, though difficult to quantify, everyone understands the benefits of secure and trusted identification. The proposed minimum standards seek to improve the security and trustworthiness of a key enabler of public and commercial life -- state-used driver's licenses and identification cards. As detailed below, these standards will impose additional burdens on individuals, States, and even the Federal government. These costs, however, must be weighed against the intangible but no less real benefits to both public and commercial activities achieved by secure and trustworthy identification.4

This is not analysis, of course. It is surmise. A few paragraphs later, it continues: The proposed REAL ID regulation would strengthen the security of personal identification. Though difficult to quantify, nearly all people understand the benefits of secure and trusted identification and the economic, social, and personal costs of stolen or fictitious identities. The proposed REAL ID NPRM seeks to improve the security and trustworthiness of a key enabler of public and commercial life -- state-issued driver's licenses and identification cards. The primary benefit of REAL ID is to improve the security and lessen the vulnerability of federal buildings, nuclear facilities, and aircraft to terrorist attack. The rule would give states, local governments, or private sector entities an option to choose to require the use of REAL IDs for activities beyond the official purposes defined in this regulation. To the extent that states, local governments, and private sector entities make this choice, the rule may facilitate processes which depend on licenses and cards for identification and may benefit from the enhanced security procedures and characteristics put in place as a result of this proposed rule.

The assessment goes on to imagine what protection-rates would cost-justify the REAL ID Act regulations.5 According to the assessment, if REAL ID lowers by 3.6% per year the annual probability of a terrorist attack causing immediate impacts of $63.9 billion, the rules would have net benefits. If REAL ID lowers by 0.61% per year the annual probability of a terrorist attack causing both immediate and longer run impacts of $374.7 billion, the rules would have net benefits.

This is an unsound way of judging the anti-terrorism benefits of REAL ID, and it reflects almost no thinking about how REAL ID might work as a security tool. I have attached as Appendix A a rudimentary analysis of the REAL ID Act in terms of risk management, using the framework put forward by the Department of Homeland Security's Data Privacy and Integrity Advisory Committee.6

To summarize, creating a national identification scheme would not just attach a known, accurate identity to everyone. It would cause wrongdoers to change their behavior. Sometimes this would control risks, sometimes this would shift risks from one place to another, and sometimes this would create even greater risks.

Rather than being evaluated on its ability to prevent attacks outright, as the NPRM did, the REAL ID Act should be assessed in terms of its ability to delay attacks or change their character. Assuming, for example, that a future attack would be on the scale of a 9/11 -- an exaggerated assumption unless all the rest of our security efforts have done nothing -- REAL ID might be assumed (generously) to delay such an attack by six months. The value of delaying such an attack, and thus the security value of REAL ID, ranges from $2.24 billion to $13.1 billion.7 REAL ID offers less in benefits than it does costs -- even using very generous assumptions.

The NPRM concludes with this:

The potential ancillary benefits of REAL ID are numerous, as it would be more difficult to fraudulently obtain a legitimate license and would be substantially more costly to create a false license. These other benefits include reducing identity theft, unqualified driving, and fraudulent activities facilitated by less secure driver's licenses such as fraudulent access to government subsidies and welfare programs, illegal immigration, unlawful employment, unlawful access to firearms, voter fraud, and possibly underage drinking and smoking. DHS assumes that REAL ID would bring about changes on the margin that would potentially increase security and reduce illegal behavior. Because the size of the economic costs that REAL ID serves to reduce on the margin are so large, however, a relatively small impact of REAL ID may lead to significant benefits.

The actual economic analysis produced by DHS and placed in the rulemaking docket has some more specific information about "ancillary benefits." It estimates that REAL ID could reduce the costs of identity theft by merely $1.6 billion during 2007-16.8 Relatively little identity fraud uses drivers' licenses. No other benefits are estimated.

In summary, implementation of REAL ID would cost over $17 billion dollars. Its security benefits, under generous assumptions, might reach about $15 billion. REAL ID promises 88 cents worth of security and "ancillary benefits" for every national security dollar we spend. These dollars would be taken from children's health care, from American families' food budgets, and from security programs that actually increase our protections. Implementing REAL ID would harm the country.

If REAL ID did add to our country's protections, it would not have been passed attached to a military spending bill two years ago. It would have had hearings, up-or-down votes in both houses, and fanfare at every step of the legislative process.

If REAL ID added to our country's protections, Americans would happily tolerate the expense, inconvenience, and intrusion created by the REAL ID system. They do not.
Securing the country is not controversial. REAL ID is controversial.

DHS Punted on the Hard Issues

The potential security benefit of having a national ID is the most important consideration. As we now see, REAL ID fails cost-benefit analysis. But there are additional costs of REAL ID that are not considered in the NPRM's cost-benefit analysis. These costs are denominated in the privacy and civil liberties of law abiding Americans.
Many states waited to see what they would find in the Department of Homeland Security's REAL ID regulations. Since DHS issued its regulations, many states have moved forward with anti-REAL ID legislation. I have attached as Appendix B a list of anti-REAL ID activity in the states since the regulations came out. On the toughest technology, security, and privacy issues, states have been left holding the bag. They do not want REAL ID, and for good reason.

Were they to comply with the REAL ID Act, states would have to cross a mine-field of complicated and expensive technology decisions. They would face enormous, possibly insurmountable, privacy and data security challenges. But the Department of Homeland Security avoided these issues by carefully observing the constraints of federalism even though the REAL ID law was crafted specifically to destroy the distinctions between state and federal responsibilities.

The Federalism Issue

The Constitution established a federal government with limited, enumerated powers, leaving the powers not delegated to the federal government to the states and people.[9] Because direct regulation of the states would be unconstitutional,[10] the REAL ID Act conditions federal acceptance of state-issued identification cards and drivers' licenses on their meeting certain federal standards.

This statutory structure -- using state machinery to implement a federal program -- is unfortunate. It blurs the lines of authority and obscures the workings of government from citizens and taxpayers. But it does draw federalism into play as a potential limit on the Department's ability to regulate.

As the Notice of Proposed Rulemaking notes,11 Executive Order 13132 says that "issues that are not national in scope or significance are most appropriately addressed by the level of government closest to the people."12 Laying out the criteria for policymaking when federalism is implicated, the Executive Order says, "National action limiting the policymaking discretion of the States shall be taken only where there is constitutional and statutory authority for the action and the national activity is appropriate in light of the presence of a problem of national significance."13

In support of a federal function -- national security -- the REAL ID Act conditions federal acceptance of state identification cards and drivers' licenses on their meeting federal standards for documentation, issuance, evidence of lawful status, verification of documents, security practices, and maintenance of driver databases. The federal government has equal power -- and the Department of Homeland Security had discretion in this rule -- to condition acceptance of identification cards and drivers' licenses on closely related priorities, including meeting standards for privacy and data security.

The decision not to do this is a policy question that, according to the federalism Executive Order, turns on whether there is constitutional and statutory authority and whether national action is appropriate. The Department's decision to abandon these issues to the states is an implicit finding that privacy and data security are not problems of national significance. That finding is wrong. Privacy is a problem of national significance.

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

The United States Government has a solemn obligation, and shall continue fully, to protect the legal rights of all Americans, including freedoms, civil liberties, and information privacy guaranteed by Federal law, in the effective performance of national security and homeland security functions.14

Among the many federal laws that are relevant is the Privacy Act of 1974.15 The Privacy Act requires federal agencies to undertake a variety of information practices, and it accords individuals a number of rights intended to protect privacy and similar interests. The law requires agencies to extend these protections to systems of records operated "by or on behalf of the agency . . . to accomplish an agency function" when that is done by contract.16

The Privacy Act did not contemplate that states would maintain systems of records in furtherance of federal functions. However, Office of Management and Budget guidelines issued after the Privacy Act's passage say that the Act is intended to cover "de facto as well as de jure Federal agency systems."17

Another relevant law is FISMA, the Federal Information Security Management Act of 2002.18 FISMA seeks to bolster information security within the federal government and for federal government functions by mandating yearly security audits. FISMA makes the head of each agency responsible for information security protections with regard to information systems and "information collected or maintained by or on behalf of the agency."19

REAL ID's Legislative History

The legislative history of the REAL ID Act suggests Congress' intention that the Department should implement REAL ID consistent with federal government policies on privacy. The Department of Homeland Security's Privacy Impact Assessment reviews relevant portions of that history:

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

DHS will be expected to establish regulations which adequately protect the privacy of the holders of licenses and ID cards which meet the standards for federal identification and federal purposes.
In addition, the Conference Report discussion of Section 202(b)(9) of the Act, which calls for using "a common machine-readable technology, with defined minimum data elements," clearly indicates that Congress wanted privacy to be a consideration in implementing the technology. The Conference Report states:
There has been little research on methods to secure the privacy of the data contained on the machine readable strip. Improvements in the machine readable technology would allow for less data being present on the face of the card in the future, with other data stored securely and only able to be read by law enforcement officials.20
REAL ID has Formidable Privacy and Data Security Problems
The privacy and data security consequences arising from REAL ID are immense, increasingly well understood, and probably insurmountable.

The increased data collection and data retention required of states is concerning. Requiring states to maintain databases of foundational identity documents will create an incredibly attractive target to criminal organizations, hackers, and other wrongdoers. The breach of a state's entire database, containing copies of birth certificates and various other documents and information, could topple the identity system we use in the United States today. The best data security is avoiding the creation of large databases of sensitive and valuable information in the first place.

The requirement that states transfer information from their databases to each other is concerning. This exposes the security weaknesses of each state to the security weaknesses of all the others. There are ways to limit the consequences of having a logical national database of driver information, but there is no way to ameliorate all the consequences of the REAL ID Act requirement that information about every American driver be made available to every other state.

There are serious concerns with the creation of a nationally uniform identity system. Converting from a system of many similar cards to a system of uniform cards is a major change. It is not just another in a series of small steps.

Economists know well that standards create efficiencies and economies of scale. When all the railroad tracks in the United States were converted to the same gauge, for example rail became a more efficient method of transportation. Because the same train car could travel on tracks anywhere in the country, more goods and people traveled by rail. Uniform ID cards would have the same influence on the uses of ID cards.

There are machine-readable components like magnetic strips and bar codes on many licenses today. Their types, locations, designs, and the information they carry differ from state to state. For this reason, they are not used very often. If all identification cards and licenses were the same, there would be economies of scale in producing card readers, software, and databases to capture and use this information. Americans would inevitably be asked more and more often to produce a REAL ID card, and share the data from it, when they engaged in various governmental and commercial transactions.

In turn, others would capitalize on the information collected in state databases and harvested using REAL ID cards. Speaking to the Department of Homeland Security's Data Privacy and Integrity Advisory Committee in March last week, Anne Collins, the Registrar of Motor Vehicles for the Commonwealth of Massachusetts said, "If you build it they will come." Massed personal information will be an irresistible attraction to the Department of Homeland Security and many other governmental entities, who will dip into data about us for an endless variety of purposes. Sure enough, the NPRM cites some other uses that governments are likely to make of REAL ID, including controlling "unlawful employment," gun ownership, drinking, and smoking. Uniform ID systems are a powerful tool. If we build it, they will come. REAL ID will be used for many purposes beyond what are contemplated today.

But the NPRM "punts" on even small steps to control these privacy concerns. It says for example that it "does not create a national database, because it leaves the decision of how to conduct the exchanges in the hands of the States."21 My car didn't hit you -- the bumper did!

As to security and privacy of the information in state databases, the NPRM proposes paperwork. Under the proposed rules, states must prepare a "comprehensive security plan" covering information collected, disseminated, or stored in connection with the issuance of REAL ID licenses from unauthorized access, misuse, fraud, and identity theft.

Requiring production of a plan is not nothing, and the NPRM refers to various "fair information practices." However, preparing a plan is not a standard. The NPRM does not even condition federal acceptance of state cards on meeting the low standards of the federal Privacy Act or FISMA.

The REAL ID Act provided the Department of Homeland Security with very little opportunity to "fix it in the regs." And DHS did not fix it in the regs. In fact, DHS created new concerns, such as the possibility of tracking by race.

REAL ID: The Race Card

The "machine-readable technology" required for every REAL ID-compliant card has been a subject of much worry and speculation. This is not without reason. A nationally uniform ID card will make it very likely that cards will be requested, and the data on them collected and used, by governments and corporations alike. DHS was wise to resist the use of radio frequency identification tags in REAL ID.22

But even more significant issues have been created by the DHS's choice of technical standards. The standard for the 2D barcode selected by the Department includes the cardholder's race as one of the data elements.
If the REAL ID card is implemented, Americans transacting business using the REAL ID card may well be filling government and corporate databases with information that ties their race to records of their transactions and movements.

For the machine readable portion of the card, the technology standard proposed by DHS in the NPRM is the PDF-417 two-dimensional bar code. According to DHS, the PDF-417 barcode can be read by a standard 2D barcode scanner.23 This is a more highly developed version of the barcode scanning that is done in grocery stores across the country.

The version selected by DHS is the 2005 AAMVA Driver's License/Identification Card Design Specifications, Annex D. This is a standardized format for putting information in the bar code. A summary of the data elements from the standard is attached as Appendix C, but briefly, white people would carry the designation "W"; black people would carry the designation "BK"; people of Hispanic origin would be designated "H"; Asian or Pacific Islanders would be "AP"; and Alaskan or American Indians would be "AI."

DHS does not require all the data elements from the standard, and it does not require the "race/ethnicity" data element, but the standard it has chosen will likely be adopted in its entirety by many state driver licensing bureaus. The DHS has done nothing to prevent or even discourage the placement of race and ethnicity in the machine readable zones of this national ID card. Avoiding race- and ethnicity-based identification systems is an essential bulwark of protection for civil liberties, given our always-uncertain future. In Nazi Germany, in apartheid South Africa, and in the recent genocide in Rwanda, horrible deeds were administered using identification cards that included information about religion, about tribe, and about race. It took 60 years for the originally benign inclusion of ethnicity in the Rwandan national ID card to become a tool of genocide, but it happened all the same. Implementation of the REAL ID Act, which would permit race to be a part of the national identification card scheme, would be a grave error.
Akaka-Sununu is Essential -- and it Needs a Vision of the

Future

Congratulations again, Mr. Chairman on your leadership in cosponsoring legislation to repeal REAL ID and restore the ID security provisions from the 9/11-Commission-inspired Intelligence Reform and Terrorism Prevention Act.
REAL ID is often touted as a direct response to a strong recommendation of the 9/11 Commission. This is untrue on a number of levels.

The recent push for national ID cards is in reaction to the terrorist attacks of September 11, 2001, of course. An appendix to a report by the Markle Foundation Task Force on National Security in the Information Age recommended various governmental measures to make identification "more reliable."24 This report was cited by the 9/11 Commission as it recommended "federal government . . . standards for the issuance of birth certificates and forms of identification, such as drivers licenses."25 But it is important to know that the 9/11 Commission devoted about ¾ of a page in its 400-page report to identification issues. Identification security was not a "key finding" of the Commission.

Nonetheless, a provision of the Intelligence Reform and Terrorism Prevention Act of 2004, passed in response to the 9/11 Commission Report, established a negotiated rulemaking process for determining minimum standards for federally acceptable driver's licenses and identification cards.26 This provision -- the result of the 9/11 Commission report -- was repealed and replaced by the REAL ID Act. Restoring the earlier, more careful provisions would be a step in the right direction.

But the Congress should examine our country's identification policies and practices even more carefully. Identification systems have many benefits but, as we know from REAL ID, they also carry many threats. We should have a much more careful national discussion about the design of the identity systems we will use in the future.
There are identification systems being devised today by the countries' brightest technologists that would provide all the security that identification can provide, but that would resist tracking and surveillance. Meanwhile, hundreds of millions -- if not billions -- of taxpayer dollars are already being spent on government ID systems with little regard for their interoperability with emerging open standards, to say nothing of privacy.

It would be unfortunate of the federal government spent so much time and money to build systems that lead in a few decades to a very costly dead end. Even worse would be for government systems to predominate, making it a practical requirement that Americans do have to carry a national ID card in order to function.

As it moves forward, I recommend that the Akaka-Sununu legislation include consideration of emerging open standards for government IDs and credentials. Rather than being locked into the unwieldy federal systems now being created, federal agencies should have the flexibility to accept any identification card or credential that meets or exceeds government standards for data accuracy, security, and verifiability.
In Akaka-Sununu, Congress should recognize the emergence of identity and credentialing systems that are diverse, competitive, and -- most importantly -- privacy protective. These systems can maximize security while minimizing surveillance. REAL ID is the ugly alternative to getting it right.

1 Executive Order 12866, Regulatory Planning and Review (Sept. 30, 1993), requires "significant regulatory actions," such as those costing over $100 million annually, to be assessed in terms of benefits, costs, and alternatives.
2 Id. at 10,845 (2006 dollars discounted at 7%).
3 National Conference of State Legislators, NCSL News: REAL ID Will Cost States More than $11 Billion (Sept. 21, 2006) .
4 See 72 Fed. Reg. 10844-46 (Mar. 9, 2007).

5 This is permitted by OMB Circular A-4 when it is difficult to quantify and monetize the benefits of a rulemaking.
6 Data Privacy and Integrity Advisory Committee, U.S. Department of Homeland Security, Framework for Privacy Analysis of Programs, Technologies, and Applications, Report No.

2006-01 (Mar. 1, 2006) .
[7] Assumed delay from today until 6 months into the future. (Net present value at 3.5%/6 months interest.)
[8] Department of Homeland Security, Regulatory Evaluation, Notice of Proposed Rulemaking, REAL ID at 130 (Feb. 28, 2007)
[9] U.S. Const. amend. X.
[10] New York v. United States, 505 U.S. 144 (1992).
[11] 72 Fed. Reg. 10,820 (Mar. 9, 2007).
[12] E.O. 13132, Federalism (Aug. 4, 1999).
[13] Id.

[14] E.O. 13353, Establishing the President's Board on Safeguarding Americans' Civil Liberties (Aug 27, 2004).
[15] 5 U.S.C. §552a.
[16] Id. at §552a(m).
[17] Office of Management and Budget, Privacy Act Implementation: Guidelines and Responsibilities.
[18] 44 U.S.C. § 3541 et seq. (enacted as Title III of the E-Government Act of 2002, Pub.L. 107-347).
[19] 44 U.S.C. § 3544(a)(1)(A).
[20] U.S. Department of Homeland Security, Privacy Impact Assessment for the REAL ID Act (Mar. 1, 2007) (footnotes and italics omitted) .

[21] 72 Fed. Reg. 10,825 (Mar. 9, 2007).

[22] The NPRM left the door for putting RFID chips in our identification cards in the future. See 72 Fed. Reg. 10,841-2 (Mar. 9, 2007). The DHS Data Privacy and Integrity Advisory Committee concluded recently that RFID is not well suited to the task of identifying people, at least at this stage in the technology's development. Department of Homeland Security, Data Privacy & Integrity Advisory Committee, The Use of RFID for Human Identify Verification, Report No. 2006-02 (Dec. 6, 2006). The Department has recently cancelled RFID-related projects. See Alice Lipowicz, DHS Tunes Out RFID, Washington Technology (Feb. 12, 2007).

[23] 72 Fed. Reg. 10,837-8 (Mar. 9, 2007).

[24] Markle Foundation Task Force on National Security in the Information Age, Creating a Trusted Network for Homeland Security (Dec. 2, 2003) . The main body of the report endorsed the finding of the Appendix unconditionally. See id. at 36.
[25] National Commission on Terrorist Attacks Upon the United States (9-11 Commission), The 9/11 Commission Report (2004) at 390.
[26] Intelligence Reform and Terrorism Prevention Act, Pub. L. No. 108-458, §7212.