WASHINGTON
LEGISLATIVE OFFICE

Testimony of Caroline Fredrickson
Director, Washington Legislative Office

American Civil Liberties Union

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

Caroline Fredrickson
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

Towards a Better Vision of Identity Documents – A Call for Congressional Action to Prevent the Implementation of a National ID System

U.S. Senate Committee on Homeland Security and Government Affairs
Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia

Hearing Regarding the Impact of Implementation: A Review of the REAL ID Act and the Western Hemisphere Travel Initiative

April 29, 2008
342 Dirksen Senate Office Building

I. Introduction and Call for Congressional Action to Repeal Real ID and Institute Privacy and Constitutional Protections for WHTI and EDLs

Subcommittee Chairman Akaka, Ranking Member Voinovich, and Subcommittee Members, Congress stands at a crossroads with respect to our national policy for identification systems. Along one path Congress can choose to do nothing and the Real ID Act will limp along for the next decade gradually creating the backbone for a National ID card system. The first path requires Congress to continuously prop up the failed Real ID program for the next decade – DHS's final implementation date is not until December 2017 – with funding and DHS cajoling. The first path necessitates the building – byte-by-byte, ID check by ID check – a de facto national ID system including the Western Hemisphere Travel Initiative ("WHTI") and Enhanced Driver's License ("EDL") systems. This choice costs billions in wasted tax dollars and threatens Americans' privacy. Or will Congress take a better path heeding the advice of states and the clear call of constituents who want ID security but not at the cost of their privacy and constitutional rights? The second path requires Congress to intervene to repeal Title II of the Real ID Act and replace it with a plan that frees states to innovate and improve ID security. It remains only for Congress to choose the correct path.

Given the tangled web of ID proposals – Real ID, Western Hemisphere Travel Initiative, Enhanced Driver's Licenses – and the unprecedented opposition to these programs, the latter choice is the only one that will advance identity security in this country. This testimony briefly discusses the two potential paths and recommends congressional intervention to avert the imposition of a de facto National ID system that offers only the fiction of security, while in fact threatening our security, vastly increasing the incidence and severity of identity theft, and that changes our culture irrevocably without any significant, measurable benefits to the American people.

On behalf of the American Civil Liberties Union ("ACLU"), America's oldest and largest civil liberties organization, its 53 affiliates and its more than half a million members, we recommend that this Subcommittee act decisively and help enact legislation, such as S. 717, the Identification Security Enhancement Act of 2007, to replace Title II of the unworkable Real ID Act of 2005, Pub. L. 109-13 (hereinafter "Real ID Act"). Additionally, we call on Congress to require that the Department of Homeland Security ("DHS") and states institute meaningful privacy and constitutional protections for the WHTI and EDL programs, or block implementation of the programs altogether.

II. Congress Must Choose Between Two Paths and Reject a National ID Card System

This is truly a moment of decision. Due to the states' unprecedented rejection of Real ID and similar systems, Congress must choose between two paths. The current path, rejected by states, would lead to the building of a National ID card system over the next decade or more. This path would bring enormous costs in the form of higher taxes, diminished constitutional rights, restrictions on individual privacy, and fundamental changes to American principles, even while providing little or no security – and even that little security coming no earlier than a decade or more into the future. The second path, represented by S. 717, requires Congress to defund and repeal Real ID. This second path is a return to the statutory language enacted by Congress in the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458. It also requires Congress to institute privacy and constitutional protections for WHTI and EDLs. This second path would prevent the creation of a National ID card system by limiting unnecessary sharing of drivers' information and safeguarding that data by maintaining state license diversity. It would free states to be innovative and dynamic in order to quickly thwart new types of identity theft and document fraud. It would lead to the enactment of cooperatively negotiated licensing standards, but with protections for privacy and constitutional rights. It is certainly cheaper and more achievable because it relies on asking the states cooperatively "what can you do?" instead of imposing upon them standards for what they must do, even where such standards are illogical or duplicative of other efforts already taken by a state to modernize its licensing system. It would also be achieved years before Real ID will ever be implemented.

The current license path leads to the eventual creation of a backbone system for a National ID card. First, all Real ID licenses would contain a standardized machine readable zone ("MRZ"), making card readers for these systems cheap and easy to deploy. Second, as will be discussed in greater detail below, the data contained in the MRZ is unencrypted, rendering it easy to capture and store. Third, the standardized formatting of data will make it profitable for third parties to capture that data with a swipe of a card both because the information is digitized and because it is presented in the same format. We can, therefore, expect Real ID readers to be present at every store and retailer in our society and at the entrance to apartment buildings and housing communities, parking garages and gyms. We should also expect that readers will eventually be placed at the entrances to many government buildings and locations. Fourth, future Congresses and state governments will find it all too convenient to require the presentation of a Real ID-compliant license to obtain any number of government services, or to exercise rights or privileges. The last two summers, Congress has already debated requiring Real IDs for obtaining federal housing assistance or federal loans, and for prescreening for employment. Finally, the interlinked

network of databases of personal information – built upon interoperable software systems – and the data verification systems – controlled by the federal government and also standardized to capture and store data – will create the data backbone for this National ID system.

Current Path:

- *De facto National ID system*
- *Enormous ongoing and upfront costs*
- *Battles over costs, privacy drag out for years*
- *Citizen nightmares at DMVs*
- *Very little visible or actual benefits to Americans.*

Akaka-Sununu S.717 Path:

- *No creation of a de facto National ID system*
- *Lower costsActual results in shorter time frame*
- *Cooperatively negotiated licensing standards*
- *Protections for privacy and constitutional rights*
- *Less political controversy*
- *Frees states to innovate quickly to stop identity theft.*

In short, if Real ID is allowed to limp forward, we will almost certainly see a ubiquitous demand for everyone to carry and present a Real ID card. It will soon serve as a de facto internal passport. Readers will proliferate and become a set of ubiquitous internal checkpoints. No one will be able to operate in modern American life without a Real ID card. Assistant Secretary Stewart Baker himself has proposed expanding the use of Real ID to require it every time an American wants to purchase cold medicine. And, the database backbone will facilitate ever increasing requests for data about every member of the public and provide a system of efficient transmission and storage of that data.

Continuation of Real ID will only ensure the extension of programs that should be terminated. If Congress does not act, Real ID will continue to force expenditures at the state level that could be used for better state-specific license or identification systems or for other needed services.

Technology vendors eager for government contracts may help propel the program forward for all the wrong reasons – leading future Congresses and/or state legislatures to expend funds merely in the name of self-perpetuation rather than due to any real and demonstrable benefit to society.

This current path would be a costly one. First, any security benefit that Real ID might provide – and security experts who have analyzed Real ID think its benefit is negligible at best[1] – will not possibly be achieved until December 2017 at the earliest – the date DHS set for states to issue compliant licenses to the whole public. It is reasonable to believe that the date of implementation may slip well past this decade-long time frame due to the technological problems inherent in establishing such an enormous, interlinked government database system, and in building the data verification systems that are required by the act.

Second, states will be forced to spend billions, and eventually the federal government will too. During the intervening decade leading up to DHS's target implementation date, software and hardware would certainly become outdated and require replacement several times over, further clouding the future of the program. States will dramatically raise taxes and licensing fees to cover the costs imposed by the Real ID Act.[2]

Third, once Real ID systems start to come on line in some states, they will become magnets for identity thieves and the best source for insiders to commit document fraud. The Real ID database will be one of the country's largest repositories of personal information on Americans, containing everything from copies of birth certificates to social security numbers. This privacy burden will be felt acutely by those drivers whose information is compromised or stolen. Meanwhile, third party retailers will be skimming information off the card and reselling purchase data to commercial data brokers who will in turn resell it to the government. This enhanced assault on our personal privacy will be shared by all of us.

---

[1] "As currently proposed, Real ID will fail for several reasons. From a technical and implementation perspective, there are serious questions about its operational abilities both to protect citizen information and resist attempts at circumvention by adversaries. Financially, the initial unfunded $11 billion cost, forced onto the states by the federal government, is excessive. And from a sociological perspective, Real ID will increase the potential for expanded personal surveillance and lay the foundation for a new form of class segregation in the name of protecting the homeland." -- Richard Forno and Bruce Schneier, "National ID Card a Disaster in the Making," *C-NET News.com*, May 3. 2007.

[2] "I think the concept, though, was that this -- like all driver's licenses -- is largely a fee-based system, and that, ultimately, the cost of building Real ID should be amortized over the driver's license fee." -- Sec. Michael Chertoff, speaking before Senate Homeland Security Committee Hearing, February 13, 2007.

Fourth, the very creation of a "real" ID will entice criminals and terrorists to acquire them so as to freely move throughout our society likely obviating any of the alleged security benefit from the Act. Experts agree that identity theft is easy to achieve. Although DHS's ID proposals appeared at first glance to provide some element of security benefit, under further scrutiny they appear to create glaring security vulnerabilities. When criminals and terrorists obtain Real ID licenses under assumed names they will walk through our society without scrutiny – just as the 9/11 hijackers boarded airplanes using lawfully obtained driver's licenses.[3]

Perhaps most importantly, our constitutional traditions of living in a free society will be diminished and our culture will change in unpleasant ways if Congress does not act. The ability to live and move throughout society freely will largely evaporate. That is the chief cost of a National ID card system. Those whose religious beliefs prevent their being photographed or require head coverings will be compelled to choose between their beliefs and participating in modern society. Essentially, we will be asking people to declare who they are at a myriad of internal checkpoints – all in the faint hope of possibly obtaining some *de minimis* security benefit. Worse still, that minimal benefit may be undercut by the ease with which criminals and terrorists can obtain forged or actual Real ID licenses using the real information of a law-abiding American.

Real ID may turn out like US-VISIT, a similarly failed program that tracks immigrant visitor entries, but still fails to track their departures, and hence provides maximum privacy invasion with minimum security. Sadly despite US-VISIT's failure, Congress has yet to end this tortured program, leaving the public to bear the burden of it. If Real ID implementation is allowed to continue, the American public could be faced with a similar yet even larger boondoggle.

The second and better path, in contrast, saves us from the imposition of a National ID card system and averts many of these costs while promising increased security of identity documents. Passage of S.717, or a similar piece of legislation, puts the nation on the second and wiser path; one that restores federal policy establishing a negotiated rulemaking procedure under the Administrative Procedures Act to cooperatively devise plans for ID security enhancements. This is the policy that Congress wisely enacted in the Intelligence Reform and Terrorism Prevention Act of 2004.

---

[3] It is the ACLU's opinion that no matter what your opinion about the security benefit of ID documents, Real ID and its progeny are now the greatest impediment to increased state ID security. Real ID's implementation is years away and yet states are holding off implementation of commonsense, achievable security measures as they await Real ID's fate.

First, S. 717 would create greater ID security than Real ID because it allows innovation in protecting state DMV databases. It also would likely avert a uniform ID card and uniform computer system. The bill would certainly lead to the erection of rigid data security to control access to data collected by DMVs. While the bill would set minimum standards for state licensing, it would allow states to innovate and add features on top of those standards. Thus, if a state were seeing a particular type of document fraud, it could add a physical or digital security feature to licenses. Because Real ID relies on a set of uniform national mandates, such innovation is prevented absent passage of a new act of Congress or regulatory modifications.

Second, passage of S. 717 would reduce costs substantially for states and taxpayers by incorporating some of the security advancements already achieved by states. Contrary to DHS's assertions, states have continuously updated their licensing systems to improve data privacy and ID security. Many of these updates would surely become the base line for a set of cooperatively agreed upon standards. Therefore, should Congress choose the second path, it will dramatically reduce costs for many states. The savings will encourage state participation and reduce the need for new tax hikes or license fees.

Third, the second path would protect drivers' privacy, and therefore makes DMV databases a less attractive target for identity thieves, criminals and terrorists. Because each state would be freed to establish its own computer security and data storage protocols, hacking into one state would not provide ease of access into other states' data. While this will not prevent malicious hacking attacks, it will limit the impact of such attacks. Similarly, states would likely choose to encrypt data on the cards and as it is transmitted between states and the federal government. This would be a substantial privacy protection that DHS has declined to endorse despite its obvious security advantages. The encryption of such information, coupled with reduced standardization would make it less likely that retailers will utilize readers when purchases are made by drivers because it will be less efficient to sort, store and resell the data of consumers. Most importantly, states will surely erect barriers to access that will make it less enticing for insider fraudsters to sell real IDs with law-abiding individuals' information to identity thieves, criminals and terrorists. And, when such fraud occurs – as it surely will – the fake IDs that were sold will not necessarily be treated as above reproach by neighboring states.

Finally, the second path would preserve the tradition of free, unfettered movement throughout society and the right for law-abiding citizens to remain anonymous. That tradition was enshrined in the Constitution, which replaced the Articles of Confederation and the series of internal ID checkpoints they permitted. That tradition has endured despite

numerous external and internal threats that have arisen since 1789 and should not be cast aside now.

III. Widespread State Opposition Requires Congressional Intervention to Prevent the Creation of a National ID System

The ACLU believes that Congress must act decisively and choose the second path because, despite DHS's recent rhetoric to the contrary notwithstanding:

- The entire Real ID Act scheme is collapsing as states recognize the unprecedented burdens on taxpayers' privacy and civil liberties imposed by this unfunded mandate, and as states enact legislation prohibiting participation.
- Rather than resolving privacy problems posed by the Real ID Act, DHS's inaction makes it likely that third-party privacy invasions will become commonplace if Real ID is ever implemented. Similarly, Congress must block the introduction of EDLs enabled with Radio Frequency Identification Devices ("RFIDs").
- DHS has largely thrown up its hands and abdicated its implementation responsibilities by not requiring states to fully implement Real ID until nearly a decade from now, at the earliest. This action belies statements that DHS believes that Real ID, WHTI and EDLs are critically important security tools.

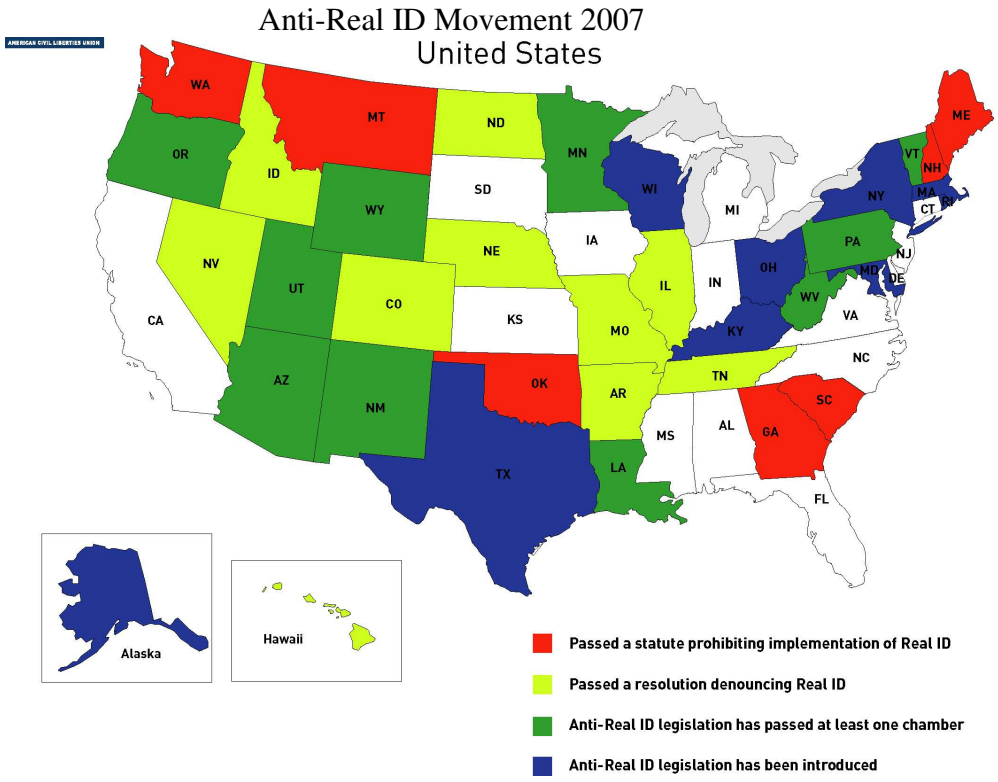
A. States Rejection of Real ID is Accelerating

Reiterating our testimony before this Subcommittee 13 months ago, one thing has become clear – states and the public are moving en masse to reject the Real ID Act and calling for Congress to repeal it in toto. That process is accelerating, not diminishing. Rather than mollifying state government officials' concerns, DHS's January publication of a fatally flawed Final Rule that largely disregarded the more than 21,000 comments opposing Real ID has set off a new round of state opposition. In response, state governments are rapidly moving to opt out of this unfunded mandate altogether.

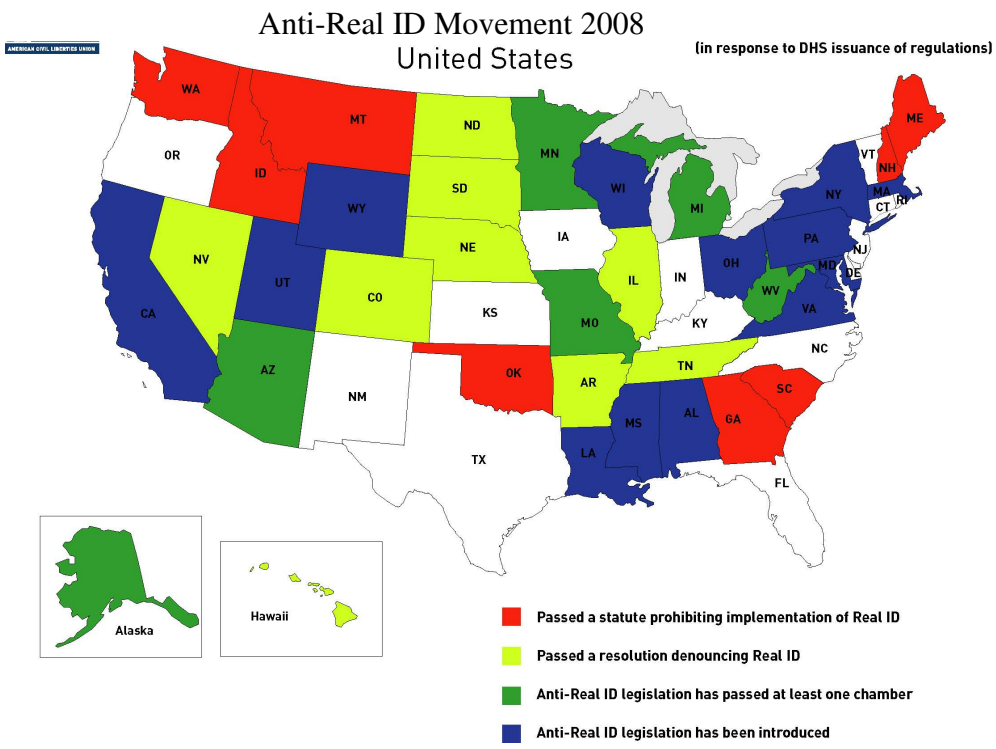
States are also refusing to comply with Real ID. States took extensions on the statutory deadline not to signal compliance but to simply run out the clock on the Bush Administration. Governor Mark Sanford (R-SC), sent a letter to every Member of Congress this month calling Real ID "the worst piece of legislation I have seen during the 15 years I have been

engaged in the political process,"[4] and urging its repeal. When asked whether Montana would participate in Real ID, Governor Brian Schweitzer (D-MT) exclaimed "No. Nope. No Way. Hell No."[5]

State opposition has led to the unprecedented passage of state laws prohibiting compliance or implementation of the Real ID Act. Governor Butch Otter (R-ID) recently signed into law an act prohibiting Idaho from implementing Real ID, HB 606. Idaho thus became the eighth state to enact such a law, joining Georgia, Maine, Montana, New Hampshire, Oklahoma, South Carolina, and Washington. Legislation is pending Governor Palin's (R-AK) signature in Alaska to prohibit funding of Real ID. Similar legislation awaits Gov. Tim Pawlenty's signature in Minnesota. Ten additional states have unequivocally stated their formal opposition, with many calling on Congress to repeal Real ID entirely. These states are: Arkansas, Colorado, Hawaii, Idaho, Illinois, Missouri, Nebraska, Nevada, North Dakota, and Tennessee. South Dakota passed a similar resolution in direct response to the release of DHS's final rule. Legislation opposing Real ID has passed at least one chamber of a state legislature in an additional 11 states.[6] In all, only eight states have not seen the introduction of anti-Real ID legislation.



[4] Gov. Mark Sanford to Members of Congress, April 3, 2008.
[5] Associated Press, "Gov. signs law rejecting Real ID act," *Billings Gazette*, April 17, 2007.
[6] Those states are: Arizona, Oregon, Louisiana, Michigan, Missouri, New Mexico, Pennsylvania, Utah, Vermont, West Virginia, and Wyoming.



States also defied DHS's demands that states seek an extension of time to become Real ID-compliant. In fact, many explicitly refused to commit to implementation of Real ID in the future. Four states, Maine, Montana, South Carolina and New Hampshire refused to request such an "extension." DHS contradicted the plain language of its own Final Rule, which allowed states to take an extension waiver as of right and without indicating an intent to commit to Real ID implementation. Yet, despite this regulatory language, DHS engaged in brinksmanship with these states and then stated that any state that received a waiver intended to implement Real ID. In a naked attempt to save face and avoid a confrontation that would surely show that DHS was unable to cajole states into compliance, DHS chose to misconstrue these states' opposition letters as requests for extensions. In response to a letter from Montana Attorney General Mike McGrath asking DHS not to enforce the statutory deadline on Montana residents, DHS Assistant Secretary Stewart Baker wrote, "I can only provide the relief you are seeking by treating your letter as a request for an extension,"[7] and then proceeded to grant Montana an extension it never requested. The California Department of Motor Vehicles felt compelled to send DHS a letter two months after the state had received an extension to clarify that it was not committing to Real ID, stating unequivocally, "California's request for an extension is not a commitment to implement REAL ID, rather it will allow us to fully evaluate the impact of the final

[7] Stewart Baker to Mike McGrath, March 21, 2008.

regulations and precede with necessary policy deliberations prior to a final decision on compliance."[8] An additional dozen states wrote or stated similar disclaimers.[9]

B. DHS's Final Real ID Rule Failed to Resolve Privacy Problems

DHS has failed to resolve the privacy-invasive potential of the Real ID Act. As we stated last year, the Final Rule undercuts Congress' earlier effort to protect drivers' information, which is considered by many to be of higher quality than commercial data amassed from warranty cards and the like. Responding to the murder of actress Amy Boyer by a man who obtained her address from the New Hampshire DMV, in 1994 Congress passed the Drivers' Personal Privacy Act ("DPPA"), Pub. L. 103-322, 18 U.S.C. § 2721, et seq., which requires such data to be kept confidentially. Every state has passed legislation to implement the DPPA. Many of these state statutes, like California's, go beyond the original act. This is in sharp contrast to the Real ID Final Rule, which provides states with no guidance on how a nationwide database should be created and how the information in it should be protected.

Despite widely acknowledged security and privacy benefits, DHS refused to encrypt the MRZ, which will lead to a thriving third-party market in data collected from swiping the card itself when packaged with detailed sales and tracking data. The standardization of the MRZ and its data elements facilitates the capture of the data on the card. Standardization makes card readers efficient. Digitization of the information in an unencrypted form invites third-parties to demand presentation of the cards. DHS's failure to prohibit third-party collection and resale encourages retailers, security companies and property managers to gather card data at a myriad of places. Already, private sector third parties have a ready market for such information through resale along with detailed sales information to data broker companies. These companies, in turn, repackage and resell the information to other companies and to federal, state and local agencies. Thus, DHS's regulatory failure to protect privacy supercharges the market for sale of private data about consumers that is tied directly to each consumer's driver's license.

---

[8] George Valverde to Michael Chertoff, March 18, 2008.

[9] See, e.g., statement on Pennsylvania Department of Transportation website (at http://www.dmv.state.pa.us/idSecurityCenter/realID.shtml): "This extension does not commit the commonwealth to implement REAL ID. The extension allows for more time to complete a comprehensive analysis of the REAL ID regulations to determine potential options, the costs involved and the affect on Pennsylvania's citizens." For additional statements, see Broach, Anne and McCullagh, Declan, "Real ID Could Mean Real Travel Headaches," *C-Net News.com*, February 4, 2008.

The DPPA would be completely undercut if Congress allows for the easy harvesting of data from both the printed information and the MRZ on the license. In fact California would need to amend state laws to reduce privacy protections as California law would be in conflict with the Final Rule. If Real ID were ever to be implemented in accordance with the Final Rule, it would be a major step backward from a good policy that protects Americans like Amy Boyer every day.

C. DHS's Actions Speak Louder than Words; DHS Is Kicking the Can Down the Road

Despite its recent act of brinkmanship with Maine, Montana, New Hampshire and South Carolina, the current DHS management's timetable for Real ID's implementation is at least a decade long, undercutting Secretary Chertoff's claims that Real ID is a security imperative. The Final Rule does not require states to issue the first Real ID-compliant licenses until December 1, 2013, and then only for drivers 50 years of age and younger. It is not until December 1, 2017, nearly a full decade from now and more than 16 years after 9/11 that states would need to issue Real ID-compliant licenses to the remainder of drivers.

For the second year in a row, the President's budget did not request funding to reimburse states for their expenses in implementing this unfunded mandate. This illustrates that Real ID funding is not a priority for DHS. Congress should see DHS's actions for what they are – an attempt to make Real ID the next President's problem rather than work through the myriad hassles bedeviling implementation. This timeline is in sharp contrast to S. 717 which would have a workable identity framework in place in two years. For this reason alone Congress should repeal the Act and start over with a cooperatively agreed upon licensing system.

IV. Limping Towards Creation of Additional Card Systems that Invade Privacy

Just as bureaucratic inertia, absent congressional intervention, will lead inexorably towards the building of a Real ID system that is the backbone of a National ID card system, sporadic movement towards implementation of WHTI-compliant licenses and EDLs will build card systems that invade Americans' privacy in new ways without adding security benefits. Through fits and starts, these programs – despite their overlapping missions and lack of clear security benefit – may be initiated and slowly propelled forward. These programs will gather detailed information that tracks the cross border movement of U.S. persons. How soon before the readers are placed at the borders between the states or at major city boundaries or near national monuments and government buildings, not just at the U.S.-Canada and U.S.-Mexico borders?

Just as we all use separate keys to secure separate locks rather than one universal skeleton key, it is good ID security to require separate IDs for separate purposes. Nevertheless, the security and privacy advantages of separate IDs are undercut when the licenses – in the name of efficiency – become linked as these three systems may soon be. Congress should resist convergence of these licenses and their computer network systems. The ACLU opposes such proposals because they will hasten the imposition of a National ID system by marrying detailed driver information with a movement tracking capability. We believe that WHTI compliance licenses work best as separate identity systems – avoiding the rigidity and security flaws inherent in a National ID system.

The Enhanced Driver's License program presents additional privacy problems. DHS requirements for EDL include the use of Radio Frequency Identification (RFID) technology, which has proved highly insecure and has even been abandoned by DHS in other contexts. RFID chips emit a radio signal that transmits data a substantial distance away. As such, they allow remote tracking of the license holder, by government officials or anyone else who buys an RFID reader over the internet. The data transmitted by RFID is also highly vulnerable to hacking and cloning. Shortly after the U.K. introduced RFID chips into their passport, a hacker cloned the chip, encoding an innocent person's data into a fraudulent passport.

The measures DHS is proposing to secure the RFID chip in the EDL would be laughable if they were not so alarming: a tin foil envelope to hold your license and an "awareness" campaign. DHS claims additional protections are not needed since all the EDL will broadcast only a unique identifying number. But that is exactly what a Social Security Number is – a unique identifying number that does not in itself contain private information about you, but can be used to access your most sensitive data. Further, the unique identifying number does nothing to prevent tracking: once someone's unique ID is learned, that number can be used to track his or her movements by anyone with a cheap RFID reader.

DHS cannot claim to be unaware of the problems inherent in RFID technology – since DHS itself abandoned use of RFIDs in the US-VISIT program because of insurmountable technological hurdles. The Department's own Data Privacy and Integrity Committee warned against using RFID for tracking and monitoring people, because of security risks of "skimming" and intercepting the signal, and the potential for broader tracking of individuals' movements and activities. EDL will do exactly what DHS's own privacy committee warned against.

The security rationale for both programs is lacking. DHS justifies these programs as promoting efficient border crossing because the cards

would permit remote clearance of border crossings. Yet, unless an agent physically compares the picture produced by a transmitting RFID with the actual occupants of a vehicle crossing the border, all the government learns is that the ID issued to a certain person crossed the border. Absent such a secondary stop and review, the government cannot know that the person who owns the license crossed with the card. Thus, the system is easy to game. If such physical stops are introduced, the speed and efficiency gains promised by using RFID-enabled licenses virtually disappear.

Furthermore, the security benefits for these programs is lacking given that undocumented immigrants, smugglers, criminals and terrorists will likely cross our borders freely at the miles of unguarded borders rather than obtain such licenses. In short, Congress must guard against allowing DHS to implement programs that produce a negligible security benefit at best and whose threat to personal privacy is substantial. If Congress does permit these programs to proceed, it should mandate substantial privacy protections to limit the negative consequences inherent in these concepts.

V. Conclusion – Congress Must Choose a Path that Prevents the Slow Creation of a Fatally Flawed National ID Card System.

Congress cannot sit idly by while the Real ID Act threatens Americans' privacy and hampers improvements to identification security. Rather, Congress must repeal the Real ID Act and, if need be, replace it with a workable, achievable statute to improve licensing security devoid of the privacy and civil liberties infirmities that hamstring the Real ID Act, and which is agreed upon by all interested stakeholders. Further, Congress should enshrine privacy and constitutional protections into WHTI-compliant Licenses and EDLs.