Through the Looking Glass

A CAGW Special Report

Real ID: Big Brother Could Cost Big Money

By: Angela French
October 17, 2005

1301 Connecticut Ave., NW, Suite 400 Washington, DC 20036
(202) 467-5300 www.cagw.org

Introduction

Sneaking through the legislative process without any congressional hearings or deliberation, the Real ID Act became law before most members of Congress had a chance to review it. Latching onto the lapels of the May 2005 emergency spending bill, the Act exploited the fears many Americans still have after September 11. Touted as an anti-terrorist and immigration reform bill, the Real ID Act has far greater ramifications than what is seen at first glance. The bill establishes strict and costly federal minimum standards for states' issuance of drivers' licenses, even though most states had already improved their methods of verifying and securing driver's licenses. It may also be a substantial and hidden tax increase for all Americans.

Local and state governments, privacy and civil rights groups, and even some members of Congress expressed outrage at the federal government's interference in state law. Rep. Ron Paul (R-Texas) scoffed at the idea that the legislation will stop terrorism or illegal immigration, and stated that "Federally imposed standards for drivers' license and birth certificates make a mockery of federalism and the 10th amendment. While states technically are not forced to accept the federal standards, any refusal to comply would mean their residents could not get a job, receive Social Security, or travel by plane. So rather than imposing a direct mandate on the states, the federal government is blackmailing them into complying with federal dictates."[1]

Some view the implementation of the Real ID Act as a chance to convince the government that the best way to secure licenses is to embed them with a tiny little chip, creating a "smartcard," which has the potential to track every movement and decision made by the cardholder. Although former Homeland Security Secretary Tom Ridge stated that the legislation that created the Department of Homeland Security (DHS) forbade a national ID card, according to Jim Harper, Director of Information Policy Studies at the Cato Institute, "The Real ID Act represents a further advance for national ID in the United States. Even though cards will be state-issued, Real ID creates a fully uniform identification system that is essentially mandatory. Real ID is the framework for a vast extension of government surveillance over law-abiding citizens."

The Orwellian plot seems far-fetched, but the government already made the mistake of mandating that U.S. passports will be updated using this technology, affecting 60 million Americans and costing $2.5 billion initially with an ongoing yearly cost of $1.3 billion to operate.[2] If the government opts to use these brittle chips, more than 196 million U.S. drivers will be forced to carry a license that has the memory to store every detail about the person, including health records, family history, bank and credit card transactions, as well as a wealth of other information.

---

[1] Rep. Ron Paul, "National ID Cards Won't Stop Terrorism or Illegal Immigration," *LewRockwell.com*, (viewed on October 12, 2005), < http://www.lewrockwell.com/paul/paul248.html>.
[2] "Passport Projects Prove That Nothing Comes Easy," *ID Trends in Personal Identification and Biometrics*, Vol. 4, No. 16, September 15, 2005, p. 2.

The additional tax burden and privacy intrusion of a chip-based driver's license would hit Americans just as they are paying more than $3.00 per gallon for gasoline and up to 50 percent more for natural gas to heat their homes this winter, on top of the hundreds of billions of dollars for hurricane relief to rebuild the Gulf Coast following Katrina and Rita. Every state and its taxpayers will be burdened by compliance costs. But the impact will be even more severe on state governments affected by the hurricanes. They will be short of revenue for some time and hard-pressed to issue a driver's license under their current system, let alone implementing the complex and expensive infrastructure required for computer chips.

A Brave New World

September 11, 2001 changed America's perceptions on protection, safety, and homeland security. The disastrous events of that day exposed the weaknesses in the federal government's ability to respond to a major national threat. In the aftermath of 9/11, the American public realized that previous protective measures put in place by the government were not enough to prevent or adequately respond to terrorist attacks.

One major flaw exposed by the terrorists was that no central database existed to allow intelligence agencies and law enforcement to communicate with one another. Responding to the lack of exchanges among the various agencies, a Federal Bureau of Investigation (FBI) official stated that "communications coming into our building from NSA, from CIA, cannot be integrated into our existing databases…. So if an analyst is working, say, on a subject in a Phoenix division and they run that person's name through our databases, they will not retrieve information on that person that other agencies may also have. It is required of them to get up, walk over to a ... different computer that has access to a different database and search that name in that database; and the two databases will never come together and be integrated."[3]

The government's inadequacies responding to September 11 also gave new life to the idea of creating a national identification card and database that could store information to allow the government to decide who may pose a threat to America's security. The scheme had been around long before September 11. But the information-sharing problems, the slow response, and the cracks in the U.S.'s intelligence world pushed the concept into the limelight.

The latest manifestation of this ongoing effort to improve the security of identification cards was the passage of the Real ID Act on May 3, 2005. President Bush signed the bill into law on May 11. The legislation implemented, for the first time, a set of federal minimum standards for authenticating and securing driver's licenses. The new system places a heavy implementation and cost burden on state and local governments, especially departments of motor vehicles (DMV), as well as taxpayers and drivers. States

[3] Dan Verton, "Report: Inadequate IT Contributed to 9/11 Intelligence Failure," *Computerworld*, July 24, 2003, (viewed on October 4, 2005), <http://www.computerworld.com/governmenttopics/government/story/0,10801,83426,00.html?SKC=news83426>.

will now have to verify birth certificates, federal immigration documents, and Social Security numbers with the appropriate federal departments, build a database to store and secure individuals' identification documents, and train personnel to use the new system. Fees and taxes will have to be increased to cover whatever costs are not paid for by the federal government.

DHS will soon set forth specific guidelines for states to implement the new federal requirements. DHS must determine which technology will be needed to implement the standards, and how to best secure the information once it is authenticated. Currently, two main forms of protection are being considered: using magnetic stripes or two-dimensional (2-D) barcodes, or embedding contactless integrated circuits such as radio frequency identification (RFID) chips into driver's licenses. Currently, 49 states[4] use either magnetic stripes or 2-D technology to protect individuals' licenses, and have had minimal identity theft problems. This form of technology is inexpensive, easily produced, and many states already use a storage system to keep the information secure.

However, installing RFID chips or similar technology into every driver's license will be an expensive, invasive, and less secure way to update identification documents. In addition to implementation expenses, states will also have to build a new system to verify, track, and store RFID information, costing a total of $17.4 billion. With governments' long history of technological ineptitude, the task is daunting. Furthermore, the extensive storage space on RFID chips allows more than birth dates and photos to be stored on the chip, posing a huge threat to privacy. Eventually, the government could mandate that additional information must be stored on the chips, including health records, travel sequencing, relatives' information, and more. Advocates tout the technology as "smart cards" as a replacement for standard drivers' licenses, but the idea is far from brilliant. Another pitfall is that information on RFID chips can be remotely accessed by unauthorized persons, therefore increasing the threat to privacy. Finally, the cost of a driver's license could rise by 260-800 percent, from $10-$25 to at least $90, a cost which will fall disproportionately on lower-income taxpayers and those on fixed incomes, including many senior citizens.

The security flaws exposed during 9/11 led many states to implement cost-effective technology to verify and protect driver's licenses, without any guidance or interference from the federal government. But, embedding RFID chips in driver's licenses is one step away from requiring that all U.S. citizens carry a national identification card. As DHS considers the best options for carrying out the Real ID Act guidelines, it should keep it simple yet secure. Before mandating a "gold plated" driver's license, it would be prudent to take a lesson from the states.

[4] 40 states use 2-D barcodes; 9 use magnetic stripes. American Association of Motor Vehicle Administrators (AAMVA), "Current and Planned Technologies for U.S. Jurisdictions," (viewed on October 3, 2005), <http://www.aamva.org/standards/stdUSLicenseTech.asp>.

The Real Deal with the Real ID Act

In response to recommendations made by the National Commission on Terrorist Attacks Upon the United States (also known as the 9/11 Commission), members of Congress began working on legislation to prevent another terrorist attack. The commission noted that identification documents and immigration laws were two vulnerable areas that needed immediate attention, and advised that stricter requirements should be imposed.

In December 2004, Congress enacted the Intelligence Reform and Terrorism Prevention Act (S. 2845), which addressed many of the commission's concerns. Included in the legislation were federal minimum standards for driver's licenses, a step lawmakers hoped would help strengthen identification document security. Prior to the bill, each state had its own criterion for securing and verifying information to issue driver's licenses. Passage of the act marked the first time federal requirements were outlined to establish secure state-issued identification documents to authenticate a person's identity.

Because the federal requirements would be implemented at the state and local levels, Congress established a committee comprised of state and federal officials to create the new set of security and verification standards. This would allow states to decide how best to bolster identification security measures while keeping costs low for local governments and taxpayers.

Five months later, Congress superseded this cooperative approach by imposing stricter, unfunded federal mandates on states in the Real ID Act. Introduced in the House on January 26, 2005 by House Judiciary Committee Chairman James Sensenbrenner (R-Wisc.), most of the provisions in the original bill (H.R. 418) made their way into the final version of the Real ID Act, which was attached to the May 2005 Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief (H.R. 1268).

Burying the Real ID Act in the emergency supplemental bill ensured that the act would pass without close scrutiny or opportunity for amendments. Rep. Sensenbrenner attempted to get some of the language included in S. 2845, but "his colleagues were uncomfortable with including the language in the Intelligence Bill passed last year" so "he was promised a second chance at passing the bill. His Republican colleagues promised that the language would be included in a 'must-pass' bill of the next Congress."[5] Sen. John Sununu (R-N.H.), in opposing the Real ID Act, stated that "'When you have a supplemental bill providing support for the troops overseas, I think it's difficult, if not impossible, to vote no…. And unfortunately there weren't a lot of people willing to stand up and say this is a bad idea.'"[6]

---

[5] "Rep. Crowley Calls Real ID Act 'Republican Abuse of Power,'" *US Fed News*, May 4, 2005, p. 1.
[6] Shawne E. Wickham, "NH Not Sold on 'National ID Card,'" *New Hampshire Union Leader*, September 18, 2005, (viewed on October 12, 2005), <http://www.theunionleader.com/articles_showa.html?article=60564>.

Although the House held discussions and floor deliberations on the Act, the provisions discussed "were ultimately not included in the act's final version."[7] The legislation was pushed through so quickly that the Senate had no time to hold hearings or debate. According to Sen. Lamar Alexander (R-Tenn.), "'This really is a national identification card for the United States of America for the first time in our history…. We have never done this before, and we should not be doing it without a full debate.'"[8] Despite a letter sent from Sens. Alexander, Sununu, and 10 other senators to Senate Majority Leader Bill Frist (R-Tenn.) urging him to block the amendment, the bill passed.

The Real ID Act usurped the ability of states and local governments to devise an effective, cost-saving system to comply with the intelligence reform mandates, which must be met by 2008. The Act will have a substantial economic impact, as states now must:

- Follow federal protective standards for locations that produce and store driver's licenses;
- Join a yet-to-be-formed interstate compact to share information with every other state;
- Meet federal data storage requirements;
- Monitor security clearances and regulate personnel training; and
- Verify birth certificates and federal immigration documents.[9]

Congress passed the legislation as an unfunded mandate; that is, without specifying any precise amount to be allocated to the states to help meet the new federal standards. However, to ensure that all states would comply with the standards without outright trampling on the 10th Amendment, Congress stipulated that a state would not receive any future federal funds if it did not follow the minimum federal standards for updating licenses. Furthermore, any identification document produced by a state that does not meet the standards will not be recognized as a federal form of identification, which, among other uses, is needed to board commercial planes and receive Social Security benefits.

---

[7] Michael John Garcia, Margaret Mikyung Lee, and Todd Tatelman, "Immigration: Analysis of the Major Provisions in the REAL ID Act of 2005," Congressional Research Service, May 25, 2005, p. 5.
[8] Erik Larkin, "Coming Soon: National ID Cards?" *PC World*, May 31, 2005, (viewed on October 12, 2005), < http://www.pcworld.com/news/article/0,aid,121077,00.asp>.
[9] National Conference of State Legislatures (NCSL), "The 'REAL ID' Act: Unworkable, Costly, and Disruptive to 9/11 Commission Reforms," (viewed on September 21, 2005), <http://www.rightsworkinggroup.org/files/NCSL_realid.pdf>.

The minimum standards for states to better secure identification documents will help authenticate identification documents. However, other specifications may have the opposite effect by imposing changes that states may be unable to implement.

For some states, bringing their driver's licenses systems up to date with minimum security necessities will be a costly endeavor; adding further requirements such as developing a new database to store information will be technologically challenging and monetarily burdensome. Ultimately, taxpayers will be saddled with the additional costs by paying more for their driver's licenses or be subject to tax increases to help offset the additional expenditures.

Currently, DHS is in the early stages of drafting guidelines for implementing the Real ID Act, and will monitor the states' progress in implementing the new requirements. Most of the requirements should be fairly straightforward, albeit time-consuming for state and local governments, especially DMVs. According to NCSL Transportation Committee Director Cheye Calvo, "state officials don't want DHS to choose one security solution for all states. They prefer trying different techniques with various business partners."[10] This strategy makes sense, as states such as Arizona and Virginia already use reliable and cost-effective technology to produce identification documents and protect them from fraud and abuse.

However, some lawmakers believe that no current license is secure enough. When the White House released its National Strategy for Homeland Security report in July 2002, "there [had] been strong interest in developing a driver's license that includes a biometric component, possibly a fingerprint."[11] But, some doubt that biometrics are enough and support a plan that calls for drivers' licenses to be embedded with RFID chips. This technology is expensive, invasive, and less secure than current methods. States will be forced to implement and pay for the technology even though many states already use dependable methods for authenticating licenses, and those that don't are facing significant upgrades in technology and training.

Lessons from the Past

There are three reasons why RFID chips are not the best solution for updating driver's licenses: technological difficulties, invasion of privacy, and high costs. Increased prices for driver's licenses and privacy issues are obvious concerns, but another reason for not choosing "smartcard" technology is that governments have a spotted past when it comes to advanced, all-inclusive software systems, which is what would be needed to produce and secure RFID-embedded licenses.

The federal government in particular has a long history of using insecure computer systems. In June 1999, Rep. Roscoe Bartlett (R-Md.) testified that the DOD computer system was penetrated more than 3,000 times, but the hackers were only

[10] Ethan Butterfield, "The Real Deal," *Newsbytes News Network*, September 10, 2005.
[11] Patrick Thibodeau, "Bush Plan Supports States in Developing Driver's License Standards," *Computerworld*, July 16, 2002, p. 1.

detected twice.[12] In 2000, hackers were able to gain root-privilege control of 155 systems at 32 federal agencies.[13]

The Federal Information Security Management Act of 2002 (FISMA) requires agencies to submit details of management and security of their computer systems. The 2004 Federal Computer Security Report Card results were released on February 16, 2005, and showed that of 24 agencies, only two[14] received an A grade, and half of the agencies received a D or F, including the Department of Defense (DOD) and DHS.[15]

The Real ID Act mandates that a system must be built to store information for drivers in all 50 states. For each driver, the database must store a scanned photo, documentation of birth, his/her Social Security number, and address. DMVs are required to contact each issuing agency (the Social Security Administration, the hospital of birth, the utility company to confirm address, etc.) to verify that the information is correct. Currently, no state has a system that can hold all of this information. Gathering and validating the information will be a laborious task itself, as the "more than 297 million birth certificates alone are dispersed across 30,000 vital records offices."[16]

The federal government has attempted to build several information systems that have been complete failures. The most costly example — in terms of dollars and security — was the FBI's Virtual Case File (VCF). After September 11, the FBI was roundly criticized for being unable to connect the dots between offices and agents, and blame was placed on its technology infrastructure. Responding to the criticism, the FBI worked to finish the VCF, which was supposed to host millions of records and be accessible to every FBI intelligence officer, field agent, and office.

The FBI began the VCF project in 2000 to replace its antiquated Automated Case System, which relies on hard copies that must be faxed or mailed between offices (so information sharing takes days rather than minutes). The VCF was expected to produce a three-second information retrieval time.

In June 2001, the FBI awarded Science Applications International Corp. (SAIC) a contract to help modernize the current system. The FBI opted to build a customized

---

[12] The 3,000 estimate is very low. Many hackers infiltrate a computer system without the agency knowing an outside person was in the system. Rep. Bartlett, testifying before the House Science Subcommittee on Technology, "Vulnerability of Government Web Sites," June 24, 1999, p. 3.

[13] Patrick Thibodeau, "Officials: Federal Systems Increasingly Falling Prey to Hackers," *Computerworld*, April 5, 2001, p. 1.

[14] The Agency for International Development and the Department of Transportation received an A grades. The House Government Reform Committee, "Federal Computer Security Report Card," February 16, 2005, (viewed on October 7, 2005), <http://reform.house.gov/UploadedFiles/2004%20Computer%20Security%20Report%20card%202%20years.pdf>.

[15] The Departments of Defense, State, and the Treasury, the National Aeronautics and Space Administration, and the Small Business Administration received Ds; the Departments of Agriculture, Commerce, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, and Veterans Affairs received F grades. Idem.

[16] Butterfield.

system from the ground up rather than use readily-available commercial software. The total cost of building and implementing VCF was supposed to be $170 million. In the interim, the FBI had no transition plan to switch from its current software to the new system, and hoped that the VCF would be built quickly and accurately.

In June 2005, *The Washington Post* obtained a confidential 32-page staff report prepared for the House Appropriations Committee. The report stated that doubts about the system were raised as early as 2003 and it "chronicles a list of errors and misjudgments that were made during the software project's troubled history, from assigning underqualified personnel to poor oversight and inadequate planning."[17]

The FBI failed to inform SAIC of its hesitancy over the system, and continued to pour taxpayer dollars into the project. By December 2004, more than 400 problems with early versions of the software had been identified, yet the bureau pressed on with a $17 million testing program even though it was clear by then that the deficient system would never work.[18]

By the time VCF was put in the junk pile in March 2005, the FBI had spent $104 million of a projected $170 million without producing a workable software system. The bureau had doubts two years prior to scrapping the project, but continued to test and build the system.

But at least the FBI terminated the project, which is more than the DOD has done with its defective, expensive, and underutilized e-travel program, the Defense Travel System (DTS).

The DTS began in 1997 when the Defense Travel System Program Management Office (DTS PMO) announced its decision to acquire a software-based travel system to take the place of traditional travel services and provide an end-to-end automated travel system. Once completed, the end-to-end system was supposed to provide every aspect of DOD's travel management needs, including travel authorization, ticketing, voucher preparation, and travel reimbursement. In this solicitation, the DTS PMO required the contractor to build a common user interface using commercial, off-the-shelf (COTS) computer software products.

Under the terms of the original contract in 1998 with BDM (which was eventually purchased by Northrop Grumman), the development, testing, and initial deployment of the travel system was required to be completed within 120 days after the contract award. The system was required to be up and running at 11,000 DOD sites worldwide by September 2001, at which time DOD personnel were supposed have a streamlined and efficient travel system. More importantly, the DTS was supposed to save money for both the DOD and taxpayers.

[17] Dan Eggen, "FBI Pushed Ahead With Troubled Software," *The Washington Post*, June 6, 2005, p. 1.
[18] Idem.

Between late 1998 and the fall of 2000, the DTS PMO began testing the system. Each batch of testing ended in utter failure. By August 2001, less than one month before DTS was to be fully deployed at all DOD sites worldwide, the DTS continued to fail its tests and was not ready for use at any DOD site. During this period it became apparent to the DOD and Northrop that DTS simply would not result in a functional end-to-end travel management system.

Up to this point, DOD had not invested any money into the program since all development, testing and deployment costs for the DTS would be covered by Northrop, as stated in the contract. Without opening the contract back up for competitive bidding, DOD and Northrop entered into negotiations and produced an entirely new agreement, violating the Competition in Contracting Act (CICA) of 1984. Instead of requiring a DTS system that operated in a client server mode (customizing and installing software in each individual computer server at every military base), Northrop only had to develop a web-based DTS, which would be similar to existing commercial Internet travel booking systems.

The most significant alteration in the DTS contract restructuring was the change to a cost-reimbursable contract, which meant that the cost and risk for development and testing was shifted from Northrop to the taxpayers, thereby eliminating any incentive for Northrop to keep its costs under control. Even worse, the government paid Northrop $53.5 million to cover the retroactive costs incurred during the unsuccessful tests prior to December 2000, and the government paid another $30-$40 million between January 2001 and March 2002, while both parties negotiated the restructure of the DTS contract and Northrop continued its fruitless attempts to make the original DTS work. Finally, the DOD agreed to pay approximately $35 to $50 million a year commencing on April 1, 2002 to continue efforts to develop a functional system using the Internet.

In July 2002, DOD Inspector General (IG) Joseph E. Schmitz released a report that estimated the costs of the DTS program had grown from the original $263.7 million to $491.9 million — 87 percent higher than the original contract amount. He found that the system would not be concluded until 2006, four years behind schedule, and severely criticized the management of the program. Despite the IG's harsh critique of DTS, DOD continued to fund Northrup's system.

The DOD's Office of Program Analysis and Evaluation (PA&E), following up on the IG's findings, released an in-depth report and cost analysis of the DTS to the DOD comptroller in December 2002. The PA&E recommended that the DOD consider commercial e-travel systems that were now available but were unavailable during the time of the original contract award to Northrop.

It is highly unlikely that a fully implemented and fully functional DTS will be achieved, even by September 2006. The most current cost estimate released in March 2005 by the Government Accountability Office (GAO) concluded that the "DTS total life cycle cost estimate, including the military service and Defense agencies, is $4.39

billion."[19] The new estimate means that taxpayers are paying $4.13 billion, or 1,565 percent, more than the original 1998 figure of $263.7 million.

However, DTS's problems do not end with rising costs and questionable functionality.

On July 26, 2004, the U.S. Court of Federal Claims, in the case of CW Government Travel, Inc. v. the United States, found that the new contract violated CICA and the change to the DTS contract was "a cardinal change," and required the DTS PMO to re-solicit the traditional travel services work.

While the court believed the DTS to be "substantially complete," it will cost taxpayers at least another $50 million to deploy the system by late 2006. The DTS that is currently deployed frequently cannot find the lowest applicable airfare available for DOD travelers, nor does it work for international travel.[20]

Considering the federal government's past attempts to build all-inclusive, unique software systems, states should be leery of the Real ID Act's requirements to build a similar network to store individuals' identity information. Designing and implementing an extensive network to track, store, and connect all information for the more than 196 million drivers in the U.S. will be a long and expensive process for states. If DHS includes unnecessary upgrades for licenses, such as extensive biometric information or chip installation, the system's requirements could become so advanced that it may never be built efficiently, much like the DTS and VCF systems.

RFID: The Orwellian Scheme

DHS is poised to hand down federal regulations that states must meet in order to issue federally-recognized driver's licenses. Post-9/11, many states began to immediately beef up security features on their own, without guidance from the federal government. In fact, according to a spokesman for Real ID Act author Rep. Sensenbrenner, "Congress actually modeled many provisions in the Real ID Act after existing standards in states including California, New York, Virginia, and Florida."[21] These and other states use several cost-effective layers of security like ghost photos and watermarks, which make counterfeiting extremely difficult and ensure that information printed on the license has been authenticated. The basic question to DHS is whether or not the federal government

[19] Gregory D. Kutz, testimony before the House Subcommittee on Government Management, Finance, and Accountability, Committee on Government Reform, "Army National Guard: Inefficient, Error-Prone Process Results in Travel Reimbursement Problems for Mobilized Soldiers," GAO, March 16, 2005, p. 28.
[20] For more on DTS, see Angela French, "Defense Travel System: The Twilight Zone of Travel," Citizens Against Government Waste, September 28, 2004, (viewed on October 3, 2005), <http://www.cagw.org/site/PageServer?pagename=reports_dts>; Thomas Schatz, testimony before the Senate Committee on Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations, September 29, 2005.
[21] Patrick Yoest, "Real ID Program May Cause Rift Between Feds, States," *Congressional Quarterly*, October 5, 2005 (viewed on October 5, 2005), <www.cq.com>.

will use inexpensive, non-intrusive, proven technology such as 2-D barcodes or a costly, invasive technology such as the RFID chip.

2-D Barcodes

Currently, 49 states[22] use either magnetic stripes or 2-D barcodes to store an individual's information on a driver's license. This technology, a security feature itself, is usually paired with watermarks, ultra-violet protection, and other enhanced security elements to ensure that the information is valid and safe. The number of states using these measures increased by 32 percent from the 37 states that used such technology when the White House national strategy report was released three years ago. Either of these options, especially 2-D barcodes with additional layers of security, is more than adequate to validate a driver's license and issue safe and secure identifications.

The use of 2-D barcodes is currently the most popular way to store information on driver's licenses because they are effective, secure, and relatively easy to produce. Information is stored along two dimensions, allowing more information to be stored than on either one-dimension barcodes (seen on food or other consumer products) or magnetic stripes (seen on credit cards). The only way to read information stored on 2-D licenses is by physically passing the license through a scanner.

Using 2-D barcodes, most licenses now carry the following information: driver's name, address, date of birth, physical characteristics, organ donor agreement, and medical impairments (such as wearing contacts or eyeglasses). Every state requires an image and signature of the driver. The 2-D barcodes also have enough memory space to allow information that is not printed on the front of the card, such as the driver's social security number or biometric information like a digital fingerprint or facial recognition. However, there is not enough space left for a large amount of additional information, such as health records or family history, allowing individuals to keep unnecessary personal information private.

States use between 10 to 20 inexpensive and effective ways to secure information on driver's licenses. The 2-D barcode itself is a protective feature used by 40 states, allowing law enforcement or other official agencies to validate that information printed on the card is authentic. Some other commonly used measures are:

- Background microtext, a variety of designs with various color patterns in the background, which "are virtually copy or counterfeit proof;"[23]

- Digital "ghost photos" of the individual, in addition to the large photo, which can be detected if tampered with;

[22] Oklahoma is the only state which does not use either of these two options. AAMVA, "Current and Planned Technologies."
[23] New York Department of Motor Vehicles, "New York's Driver Licenses," (viewed on October 4, 2005), <http://www.nydmv.state.ny.us/broch/c51A.htm>.

- Digital watermarks are covert, machine-readable features designed to deter counterfeiting and enable a variety of inspection applications;

- Printing a state symbol in ultra-violet (UV) ink over portions of information printed on the license, such as the name, date of birth, and photo; the seal will show a break if tampered with under UV black light; and

- Security laminate, an optical variable device that reflects light, making a curved line visible to the naked eye, but which is exposed if the document has been tampered with using a retro-reflective device.

RFID Technology

RFID technology has many valuable uses. The federal government and the private sector already use RFID chips to track and identify materials, including weapons, baggage on flights, cargo, nuclear materials, animals and pets, and other assets. RFID chips are used to make the highway system more efficient through tags attached to an automobile's windshield so that toll systems can easily collect payments.[24]

RFID chips are contactless integrated circuits that provide "identification and tracking capabilities by using wireless communication to transmit data."[25] The chips can either be attached to or embedded in an object, allowing scanners to theoretically read the information from as far away as 30 feet, although a distance of 10 to 20 feet is more accurate.[26] So if one individual passes another in the hall, on the street, or while standing in line, the information printed on his/her driver's license could be read without the person ever knowing his/her privacy was being violated. An identity thief can steal someone's statistics in just a few seconds by purchasing a device, often mobile handheld scanners, for less than $500 that can examine objects quickly and have the ability to read several items at once. In fact, an RFID reader (scanner) can "communicate with the tag without a direct line of sight, depending on the radio frequency and the type of tag (active, passive, or semipassive) used."[27]

There are three types of chip memories, which dictate how much of a person's identity may be stored: read-only, read-write, write-once read-many. Read-only tags have very little storage room and hold permanently entered data that cannot be altered, making them ideal for library and video rental cards. Typically, these types of tags are "passive"[28] tags, which cannot initiate communication with a scanner and can be read from about 10 to 20 feet away. Costs for passive tags range from 20 cents to several dollars, depending on the amount of memory and design. Passive, read-only tags are the most likely RFID technology that would embedded into a driver's license.

[24] GAO, "Radio Frequency Identification Technology in the Federal Government," May 27, 2005, p. 12.
[25] Ibid, p. 1.
[26] Ibid, p. 14.
[27] Ibid, p. 17.
[28] Some passive tags have large storage capacity, allowing additional data to be included. Ibid, p. 14.

Read-write tags have enough memory capacity to allow the records to be updated if necessary. These type of tags are either "semipassive" or "active," operate on an internal battery, can be read up to 750 feet,[29] have extensive storage space, and cost anywhere from $2-$20 or more. Write-once read-many chips allows information to be implanted once with no further alterations.

The radio frequency choice is a key component and "largely determines the speed of communication and the distance from which the tag can be read."[30] With every level, high-frequency tags can be read with greater accuracy and at a further distance. The four main frequencies are as follows:

- Low-frequency is best for short-range communications as it can only be read up to 1.5 feet away; it is used for items such as animal identification and antitheft systems;

- High-frequency has an accuracy range within three feet and is most often used for clothing items tracking, library and bookstore materials, and protected building access;

- Microwave frequency can be read up to three feet and is frequently used for supply chain management; and

- Ultrahigh-frequency can be read within three to fifteen feet, but the chips are more sensitive to environmental factors than the other three frequencies; passive ultrahigh-frequency tags have a rapid reading rate, and are used by several private companies and the Department of Defense.

While the technology is useful and can be relatively inexpensive, installing RFID chips into driver's licenses is overkill. The technology can be easily destroyed, simply by throwing the chip-embedded object into a microwave for 10 seconds or taking a hammer and crushing the tag. A person's identity could be wiped away with two pounds of a hammer, requiring them to pay for another license. Furthermore, it is not known how long the chip will last, and a driver may have to pay an exorbitant fee yearly or every two years because the RFID chip did not survive.

Unlike the 2-D technology, there is only one way to protect an RFID chip from unwanted readers: encryption. However, the federal government is not protecting the new U.S. passports, which will have chips, and has no plans to encrypt licenses, leaving Americans exposed and ripe for identity theft.

[29] Semipassive tags can be read from up to 100 feet away and cost between $2-$10; active tags can be read from a distance of 750 feet and have a price tag of at least $20. Idem.
[30] Ibid, p. 17.

Privacy Concerns

Privacy groups from both sides of the political aisle are concerned that the federal government will not limit use of RFID technology to storing a driver's information, but could eventually add a wealth of other data, such as health records (for instance, how many visits to and from hospitals or mental facilities), banking and credit card reports, family history, and a multitude of other personal material. Responding to the State Department's decision to embed RFID chips into U.S. passports, Electronic Privacy Information Center Fellow R. P. Ruiz stated that "RFID technology is a scary choice when it comes to electronic identification" and asked, "'Why the heck is this not a contact card?'"[31] Other groups that have opposed the use of RFID technology in government-issued identification documents include the American Association of Motor Vehicle Administrators, AARP, the American Civil Liberties Union, the Cato Institute, the Liberty Coalition, the National Governors Association, and the Service Employees International Union, to name a few.

Security experts question whether the federal government will be able to protect the new "national ID system"[32] against ID thieves. They point out that there are ways to secure the information from thieves (such as building multiple firewalls), but trusting the government, especially DHS which has received four consecutive F grades on the FISMA scale, is not the best solution.

Those favoring RFID technology are careful not to call the chips actual RFID tags. In fact, according to DHS Director of Authentication Technologies Joseph Broghamer, the department prefers "'that the terms 'RFID,' or even 'RF,' not be used at all (when referring to the RFID-tagged smartcards). Let's get 'RF' out of it altogether.'"[33] To keep privacy activists at bay and U.S. citizens from fearing the technology, RFID supporters are attempting to make a distinction between technology used for toll roads or tracking cargo and the technology that could be used for government-issued IDs even though it is one and the same. Instead, government and RFID suppliers refer to RFID tags as "contactless chips," "contactless integrated circuits," or "proximity chips," and have branded RFID-embedded IDs as "contactless smartcards."

The government should not even suggest using a technology that could track a person's movements as if U.S. citizens were nothing more than a head of cattle. The current methods used by most states are cost-effective, safe, and non-invasive. The 2-D technology allows DMVs to verify and store information to guarantee that the cardholder is holding the correct identification without storing unnecessary additional information, such as health and travel records, or family history. While no security system is

[31] Erin Biba, "Biometric Passports Set to Take Flight," *PC World*, March 21, 2005 (viewed on October 6, 2005), <http://www.pcworld.com/resource/printable/article/0,aid,120112,00.asp>.
[32] Lisa Vaas, "Analysts: 'Real ID' Act Could Help ID Thieves," *eWeek*, May 6, 2005, (viewed on October 6, 2005), <http://www.eweek.com/print_article2/0,1217,a=151449,00.asp>.
[33] Mark Baard, "RFID Cards Get Spin Treatment," *Wired News*, March 28, 2005, p. 29.

completely secure against hackers, the layered security method that most states are using make it much more difficult to steal or copy the information.

On the other hand, embedding a little gold chip into driver's licenses is not only expensive and pointless, but would be the next step toward establishing a national ID program. The federal government already made the wrong choice by approving embedding unprotected RFID chips with biometric information (a digital facial image) into U.S. passports by December 2007, affecting the security and privacy of 60 million Americans. Forcing 196 million drivers to carry a "smartcard," which can hold more information than needed on a license and can be read from a distance, could be one of the most dangerous and expensive decisions made by the federal government.

A $17 Billion Decision

Privacy groups oppose RFID-tagged licenses for fear of the federal government invading the private lives of citizens. State and local governments are resisting the RFID option because of the unnecessary costs imposed on states, and pointless regulation by the federal government. State governments and taxpayers will be burdened enough with meeting the basic Real ID Act requirements without additional RFID costs.

In February 2005, Brittan Elementary School in Sutter, California forced its 600 students to wear a RFID-tagged ID badge to "streamline the taking of attendance, giving teachers a few minutes more each day to teach and boost accuracy."[34] Parents and local civil rights and privacy groups were outraged at the idea, which propelled state Sen. Joe Simitian (D) to introduce legislation banning RFID technology to be used on any state identification document. California is not the only state resisting "smart" options: 11 other states have some form of RFID legislation on the agenda.[35]

States know which technologies work and which do not. Currently, DMVs produce roughly 72 million licenses a year, while the young and untried DHS has never managed or made IDs on this massive level. Most states today use 2-D barcodes because it is reliable and cost-effective. Using current methods, most states produce verified, protected licenses for approximately $1.50 each, keeping costs low for taxpayers. Most drivers pay between $10-$25 for a license. The RFID tags that could be embedded in licenses are estimated to cost approximately $2-$5, a seemingly low cost increase. However, the true cost for this option lies not with the actual cost of the chip, but issuing and verifying new licenses and building a database to store the information, and maintaining, training, and operating the system.

Building a database which will verify, track, and store basic information for the approximately 196 million[36] drivers in the U.S. will be an expensive and laborious task. Embedding licenses with RFID chips is unnecessary, costly, and an additional burden on

[34] Eric Bailey, "Town Gives Brave New World an 'F,'" *Los Angeles Times*, March 2, 2005, p. 1.
[35] "Passport Project," p. 6.
[36] The 196 million drivers estimate is based on 2003 Department of Transportation figures. The number has most likely increased in the past two years.

states. Also, since most states use multiple layers of reasonably priced, secure protection on issued IDs, the government should model its regulations on states that have exemplary methods of verifying and issuing drivers' licenses. More regulations and procedures handed down by the federal government may slow the progress that the states are making independently.

Since Congress passed the Real ID Act, the estimates vary for how much the mandates will cost states and taxpayers. In February 2005, the Congressional Budget Office (CBO) anticipated that H.R. 418, the original Real ID Act, would cost states approximately $100 million over five years "assuming appropriation of the necessary amounts."[37] CBO also estimated that DHS would reimburse states about $20 million over the five-year period for the cost of meeting the Real ID Act requirements.

CBO assumed that current methods would be used to implement Real ID specifications. According to CBO, DMVs will have to authenticate "proof of identification, residency, and citizenship status. Many of the agencies that issue those documents charge a fee for verification services. Licensing agencies also would have to upgrade computer systems to verify documents and to digitize and store electronic copies of all source documents. Finally, some states that do not currently require background checks for certain employees would face additional costs to complete those checks."[38]

Even assuming that the government will allow states to continue using current methods of issuing licenses, $100 million estimate is woefully low. In the spring of 2005, Washington state conducted an extensive analysis of the implementation costs of the Real ID Act. The state assumed that its current digital photo documentation and security methods would be adequate, that the federal government would provide inadequate funding and that other driver licensing authorities would not charge additional fees for document verification in other states. In its study, Washington found the following components the most costly: scanning, verifying, and retaining more documents, keeping lines short for customers, informing the public of the new system, and hiring more DMV employees.

Based on these assumptions, Washington estimated that it will cost $97 million in the first two years to implement the new regulations, $3 million less than the CBO estimated for the cost for all 50 states over five years. The forced upgrades will foist the additional costs on taxpayers, either by a general state tax increase or by directly increasing the price of a driver's license. Washington state assumed that based on its projections, drivers will have to pay $58 for a license, a $33 or 132 percent increase from the current $25 driver's license.

These estimates assume that the current demand for licenses will remain the same. Some drivers may not want a new license under these regulations, or may not be able to

[37] Congressional Budget Office, "H.R. 418, REAL ID Act of 2005," February 9, 2005, (viewed on October 10, 2005), < http://www.cbo.gov/showdoc.cfm?index=6072**&sequence=0**>.
[38] Idem.

afford it. Or, the government may force states to use RFID chips, which would require new and much higher state cost estimates.

Pennsylvania estimated that it will cost $100 million to implement the Real ID standards in its state, and Virginia calculated that it will cost $232 million ($167 million to implement the changes, and $66 million in ongoing maintenance and operation costs). CBO's five-year, $100 million estimate will barely cover one state's costs. Pennsylvania, Virginia, and Washington all use 2-D barcodes and multiple security layers to authenticate information. For states which have very few security features and do not have any storage system, the costs will be much higher.

NCSL estimated that it will cost $9-$13 billion over six years for every state to comply with the Real ID Act regulations using current license issuing techniques. Using NCSL's conservative figure, U.S. drivers can expect to pay on average a minimum of $47 for a new license, although some states (such as Washington) are already calculating higher costs.

However, if DHS requires RFID-embedded licenses, costs for states will skyrocket. The United Kingdom (UK) government may implement a national ID program using RFID technology, which could be very similar to an RFID license or a future U.S. national ID card.

In June 2005, the London School of Economics and Political Science (LSE) released its findings on an extensive six-month research project that studied the cost and implications of implementing a national ID program using RFID-embedded cards. The LSE found that the UK government's proposals for a national ID card are "too complex, technically unsafe, overly prescriptive and lack a foundation of public trust and confidence."[39] The study also found that the national ID database "may itself pose a far larger risk to the safety and security of UK citizens than any of the problems that it is intended to address."[40]

The LSE study outlines problems and costs that the U.S. can expect if DHS requires that states issue RFID-tagged licenses. The UK government proposed a national identification system to combat problems that the U.S. hopes to control by updating drivers' licenses: prevention and tracking of crime and terrorism, immigration control, and preventing identity fraud. UK and U.S. government, technology, and public awareness are similar; therefore, the LSE study is a comprehensive analysis that the U.S. federal government should consult before choosing the "smartcard" option.

Like the Real ID Act, the UK government has proposed vast updates to current identification documents, requiring a system to be built to store all the information. The UK's database would be similar to the U.S. requirements to verify, track, and store information for its citizens. Any person over 15 years and nine months would be

[39] LSE, "The Identity Project, an Assessment of the UK Identity Cards Bill and Its Implications," London: the Department of Information Systems, version 1.09, June 27, 2005, p. 5.
[40] Ibid, p. 11.

required to have a national ID card, which would affect 67.5 million citizens. "Foreign nationals" and those on extended stay would also be required to register for a national ID card. Although the UK government assumes that the smartcards would last for 10-13 years, the LSE found that the cards will wear out after 3-5 years, if they have not been lost or stolen in that time frame, increasing the cost for UK taxpayers.[41] The cost estimates for both a UK and U.S. card also vary depending on the RFID technology used.

Using the LSE's conservative cost projections, it would cost $17.4 billion to implement RFID technology and license updates in the U.S. The majority of the costs will be handed down to the states, and ultimately taxpayers. Dividing the sum, each state will have $348 million worth of costs, $168 million of which are unnecessary expenses.[42] This in turn will drive up the cost of licenses. If all costs are passed off to drivers, a driver's license will go from the manageable $10-$25 price range to roughly $90 per card, a 260-800 percent increase. Some states may choose to implement a general tax to help offset some of the additional costs of the Real ID Act, forcing non-driving citizens to pay for the federal mandate.

If DHS mandates that RFID chips be embedded into licenses, the U.S. will be one step away from a national ID program. Approximately 65 percent of the U.S. population has a driver's license; if the U.S. implements a national ID program, the implementation and maintenance costs would significantly increase.

The chart below details the specific costs for implementing, issuing, verifying and maintaining a drivers' license system for 196 million drivers using RFID technology.

[41] Ibid, p. 226.
[42] Using NCSL's conservative estimate, each state is facing an average cost of $180 million to implement Real ID standards using 2-D barcode technology. The $168 million is the estimated cost increase to issue and maintain RFID-embedded drivers' licenses.

Cost Estimates[43]

Issuing Identity Cards[44]

Action	*$ in millions*
Initial costs, including establishing guidelines, audits, and rare cases	$ 14
Purchase of biometric smartcards for 196 million drivers	$1,381
Printing personal information on cards	$ 25
Renewal of cards, assuming DMVs will issue cards every four years	$2,073
Re-issuing of cards[45]	$ 613
Total Issuance Costs	**$4,106**

Drivers' Licenses Readers[46]

Action	*$ in millions*
Purchase of readers for public sector	$ 456
Interfacing readers with national ID system	$ 52
Total Readers Cost	**$ 508**

Building the Identification Database

Action	*$ in millions*
10-year contract to build system[47]	$ 520
Deployment and updates to database	$2,202
Total contract cost	**$2,722**

Managing the National ID System

Action	*$ in millions*
Enrollment of U.S. drivers, including set up costs and logistics	$1,037
Maintenance and overhead expenses	$1,062
Information updates[48]	$ 355
Verify biometrics information	$3,369
Regular data integrity checks, compliance with Real ID Act guidelines	$ 93

[43] Cost breakdowns and estimates are based on the LSE report, which assume a 10-year implementation process. Most states have an issuance period of 4-6 years; the Real ID Act mandates that all states reissue at least every eight years, so states cannot extend issuance to 10 years. The figures do not take into account current state databases that may be upgraded to meet the federal requirements. Ibid, pp. 301-303.

[44] All issuance figures are based on a need for 196 million cards. States currently have an issuance rate of 72 million licenses annually; this figure will change upon full implementation of Real ID Act requirements.

[45] The LSE report assumed that reasons to re-issue cards include: projected defective rate of .25 percent; change of an individual's circumstances from application to processing phase; data errors; damaged cards; and lost or stolen cards. Ibid, p. 301.

[46] The UK government assumes that national ID card readers will be installed at various public locations, including airports, train stations, possibly banks, etc. The U.S. would have to install readers at similar areas as well as areas issuing the licenses. The LSE estimates are most likely lower than U.S. numbers would be.

[47] The contract estimates include: research, analysis, and development of the database; security costs; hardware and software purchases; replacement and failures of technology implemented; technology department operational costs; and risk margin. Ibid, p. 302.

[48] The LSE study assumes regular updates will be made, including: a driver's change of circumstances; verification of biometrics information; and validating the new information. The numbers are based on a much lower figure (67.5 million) than the U.S. estimates would be. Idem.

Enforcing enrollment of U.S. drivers	$ 325
Re-enrollment for altered biometrics[49]	$ 355
Identifying fraud	$ 75
Managing the National ID System	**$6,671**

Staff Costs for a 10-Year Period

Action	*$ in millions*
Training for security, use of systems, management, background checks and DMV staffing for initial deployment	$1,463
Upkeep for national database	$1,419
Training for database access and using biometric/RFID readers	$ 119
Miscellaneous costs (consulting fees, design and feasibility studies, etc.)	$ 38
Staff Costs	**$3,381**

Final Costs

Final Costs	*$ in millions*
Total Cost to implement RFID technology	**$17,388**
Cost share for each state	**$ 348**
Cost for each of the 196 million drivers	**$ .0009**

Based on foregoing analysis, the RFID option will cost states a minimum of $348 million, meaning that the 196 million drivers in the U.S. will pay approximately $90 for a license. Drivers are already facing an increase from $10-$25 per license to an average of $47; asking drivers to pay $90, or 52 percent more than the cost of 2-D barcodes, is avoidable.

States that do not have adequate technology and security methods now will be faced with even higher expenses to update their current information in order to comply with the Real ID Act guidelines. DHS should keep costs and technology difficulties to a minimum by choosing to use cost-effective and proven methods that are being used in most states today. If the chips fall where they should, they will not be included in any American's ID card.

Conclusion

Backdoor negotiations and riding on the coattails of a military spending bill allowed the Real ID Act to slip past Congress without careful scrutiny. The Act imposes stringent and costly mandates on states to update drivers' licenses, which a majority of states had begun to do prior to the legislation. Furthermore, the Act allows for additional federal interference in state and local governments' matters. Perhaps the most egregious repercussion of the Real ID Act is that it is one step closer to a national ID card program.

[49] Biometric alterations include authenticating prior information, collecting new information, and auditing for verification. Idem.

Unfortunately, states and taxpayers are stuck with the burdensome bill. As DHS decides specific guidelines for states to implement the new federal standards, the department should consider the numerous drawbacks of choosing RFID-embedded licenses: high cost, technological difficulties, unprotected data, privacy concerns, and resistance from state DMVs. Instead, DHS should opt for 2-D barcode technology paired with a wide range of additional linked and layered security features. Forty states already use this taxpayer-friendly method to verify, issue, and protect drivers' licenses.