Improving Security *and* Protecting Privacy

Through REAL ID

May 8, 2007

Executive Summary

Originally intended to certify competency to operate a motor vehicle, the typical American's driver's license today is used in the course of everyday activity as the most convenient and reliable document to authenticate personal identification. A driver's license is used to open a bank or credit account, to pay a retailer by check, to enter a commercial or government building, and to pass through security at airports and train stations. More than 80 percent of citizens use their driver's license for purposes beyond driving.

Unfortunately, the value of a driver's license as a means of identification – combined with new technologies that facilitate the copying, forgery, fabrication and exchange of fraudulent driver's licenses – have benefited underage drinkers and smokers, criminals, and terrorists. Recognizing this danger, many states took action to inhibit forgery and tighten procedures for issuing driver's licenses. Then the use of fraudulent driver's licenses by the terrorists responsible for the tragic consequence of 9-11 compelled the federal government to develop safeguards for driver's license, as enacted by Congress in the REAL ID Act on May 11, 2005.

Two years later – and more than five years after 9-11, the debate continues to smolder over imagined threats to personal privacy from REAL ID. This ITAA White Paper outlines the background of the issue, explains how proven information technologies will improve security and integrity of American driver's licenses while also enhancing privacy protections for driver's data at every level.

ITAA strongly advocates federal and state government implementation of REAL ID without further delay. ITAA also offers other recommendations for the consideration of federal and state officials to ensure that security and privacy are maintained for future generations.

Evolution of the Driver's License

The earliest known driver's license in the United States was issued in 1903 in Massachusetts to help regulate the use and ensure the safety of the new technology of transportation by automobile.[1] By the 1930s, most state agencies had joined the Bay State in licensing their drivers. To qualify for a driver's license, applicants demonstrated the basic knowledge and skills required to safely operate a motor vehicle and were issued a "license" attesting to that fact. Early licenses were paper-based, with no photos or other security features. States began to add film-based photos in the late 1950s, and driver's licenses increasingly came to be used as a means of personal identification.

Today the state-issued driver's license is the most often used and most widely accepted identity document used to establish the holder's age and residence, make use of a check for payment, open a bank account, obtain credit, enter government and commercial buildings, board a plane, get a library card, and provide access to a wide array of other services and privileges – far beyond its intended purpose to certify an individual's qualifications to drive a motor vehicle. An April 2002 poll found that 83 percent of American citizens use their driver's license for purposes beyond driving.[2] Hence the driver license has become the *de facto* identification of choice used daily by most Americans. This makes it an extremely valuable document whose security is essential – along with the abilities to authenticate it and to share its information between law enforcement across jurisdictions. These requirements reflect the mobility of Americans, the widespread use of driver's licenses for purposes other than driving, and the growing abuse and costs to the public of illegally obtained driver's licenses.

Technology as Friend or Foe

Technology has advanced by leaps and bounds since that first driver's license was issued more than 100 years ago. As an unfortunate consequence, today's driver's licenses and their rightful owners have fallen victim to theft, forgery, and counterfeiting precisely because the driver's license *has* become such a valuable document for identification. New technologies in digital imaging and printing have made false driver's licenses easier to fabricate, and the Internet provides ready access to hundreds of vendors who sell ready-made fakes online.

This rise in counterfeiting has contributed significantly to the troubling growth of one of the most common and egregious violations of personal privacy – identity theft. According to a 2006 Federal Trade Commission report, consumer complaints of identity fraud and theft increased 25% between 2003 and 2005,[3] with total economic losses to consumers of approximately $5 billion and a total cost to businesses of over $48 billion. In addition to the financial loss, it is estimated that last year it took consumers approximately 297 million hours to resolve identity theft issues.[4] Fraudulent driver's licenses also enable illegal driving and underage drinking and smoking, and as Americans have become sadly aware, terrorism and other criminal activities.

As the tragic events of Sept. 11, 2001, demonstrated, our enemies will take full advantage of any loopholes and lax security in the issuing and authentication of driver's licenses. By one report, the 9-11 hijackers had obtained a total of 17 driver's licenses.

Some had duplicate driver's licenses. Backed up with other fraudulently obtained identification, the driver's licenses enabled the terrorists to use bank accounts, take flying lessons, rent cars and pass through airport security freely. This evidence led the 9-11 Commission to state in its final report:

> Secure identification should begin in the United States. The federal government should set standards for the issuance of birth certificates and sources of identification, such as drivers' licenses. Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists.

Real ID is a direct result of these recommendations**.**

Restoring Security to Driver's Licenses

Well *before* the tragic events of 9-11, many state motor vehicle agencies had begun implementing changes to make driver's licenses more secure against the threat of identity theft and fraud through the use of digital photographs, micro-printing, barcodes, banknote style printing and other overt and covert security features. In September 2000, state representatives to the American Association of Motor Vehicle Administrators (AAMVA) voted 49 to 2 to institute the Driver License Agreement (DLA) in an effort to establish standards that would ensure a "One Driver, One License, One Record" system. In August, 2002, state representatives voted 48 to 3 to enhance the DLA by adding more security requirements. In 2004, a revised DLA was issued to and accepted by the states.

In the wake of 9-11, the U.S. government sought to expedite the *pace* of this change through federal standards that will migrate to more secure driver's licenses that will protect citizens' privacy and enhance national security.

<u>Authentication and processing</u>

The REAL ID Act, if implemented along the lines of the current Notice of Proposed Rule Making (NPRM) from the Department of Homeland Security, will substantially tighten both the data security and physical security requirements of state motor vehicle and driver's licensing offices, thus enhancing personal privacy by battling identity theft and fraud. REAL ID requires states to take new steps to verify the identity of applicants before issuing drivers' licenses and other ID cards. By December 31, 2009, state agencies will have to verify and authenticate birth certificates, social security cards and other source documents that individuals use to obtain drivers' licenses.

Although some states already have rigorous identity authentication procedures for enrollment of driver's license and other identification card applicants, the lack of minimum standards currently means that a state with insufficient or inconsistent procedures to authenticate applicants sets a lower denominator compared to states with better procedures. This attracts criminals and other abusers who can learn very easily which states have more lax requirements. The REAL ID Act sets clear requirements for

all states to ensure that documents presented to prove applicants' identities are authenticated. The documents standards for issuing a REAL ID driver's license or identification card will require states to improve fraud detection and to expedite authentication through verification from source document issuers. Technology enabled document and knowledge-based frameworks will facilitate this process until federal databases are online and fully available for authentication checks.

REAL ID also will require state authorities to share information with each other and to verify applicant data against existing federal databases such as the Social Security Administration, a step already taken by many states today. The DHS NPRM emphasizes the commitment to a "federated querying service" through which the states can access the federal reference databases in a "timely, secure, and cost-effective manner." However, DHS itself will not operate this service, and states can decide to go directly to the federal databases or use the existing AAMVANET service – a secure network owned and operated on behalf of state motor agencies by their professional association, the American Association of Motor Vehicle Administrators (AAMVA).

In addressing data sharing, *REAL ID does not establish or constitute a central, national database*, as many critics assert. To the contrary, it states a preference for a "pointer system" and assigns to the states the requirement to determine how they can best establish and secure linkages between themselves. The law, along with Senate-drafted conference language, directs the states to link their data systems to allow automated communication so that information contained in one state's system can be confirmed quickly by another.

Data exchange between states

Today a state's motor vehicle agency's computer system communicates with national systems such as the National Driver Register Problem Driver Pointer System, Social Security Administration and Commercial Driver License Information System to verify certain data, enforce safety programs, and keep records up to date. State motor vehicle data bases are closed systems (in contrast to open information systems searchable on the Internet) and access is limited to authorized users. The systems often are built on custom-developed data models and architectures with layered security components including "firewalls" to prevent unauthorized access via data links to these systems. The security access controls and firewalls, together with system intrusion detection software and audit capabilities, assure the safety of driver record information. The record shows that the data systems and computer programs associated with driver's system records are safe and secure, with an exemplary record of data security. Through the use of audit trails, a state can monitor access to information and prevent unauthorized data exchanges.

Unfortunately, gaps and vulnerabilities exist when it comes to sharing information from state to state. Although states use the Commercial Driver License Information System (CDLIS), the National Driver Register (NDR) or other programs to prevent duplicate or fraudulent licenses these systems only cover certain types of licenses and people intent on committing fraud exploit loopholes and the differences in state practices to obtain a false driver's license.

REAL ID will increase the barriers to issuing multiple licenses with real or fictitious information to the same person. To accomplish this, REAL ID requires all states to exchange certain data with all other states. At the same time, in its NPRM, DHS defers to the states to determine the design of the system to facilitate coordination between jurisdictions while safeguarding personal information. As stated in the NPRM:

> The proposed rule seeks to address many of these (privacy) issues by leaving the operation of this data query, including the development of the business rules, to the States. The rule proposes to require individual States to document their business rules for reconciling data quality and formatting issues and urges States to develop best practices and common business rules by means of a collective governance structure.[5]

REAL ID security requirements also will make these driver's licenses and other IDs tamper-resistant and harder to forge.

Further Improving Privacy Through REAL ID

In its Notice of Proposed Rule Making (NPRM) on the REAL ID Act, the Department of Homeland Security makes its commitment to privacy very clear:

> DHS believes that protecting the privacy of the personal information associated with implementation of the REAL ID Act is critical to maintaining the public trust that Government can provide basic services to its citizens while preserving their privacy. DHS recognizes the significant privacy issues that are associated with the Act.[6]

Where state-level systems are working well, REAL ID does not interfere with existing systems and procedures to protect privacy and ensure security. For example, REAL ID encourages the continuing use of the Commercial Driver License Information System (CDLIS) and the National Driver Register (NDR), whose data security records are unblemished. None of the opponents of the REAL ID Act and implementing regulations have raised a question about the protection of driver's license privacy in these systems.

REAL ID does take other important steps to *improve* the privacy protections of state driver's license applicant records, all within the existing authority of the federal government. The NPRM requires the states to report how they will maintain both data security and the physical security of the facilities where data is stored:

> "…as part of the State certification mandated by section 202(a)(2) of the Act, each State will be required to prepare a comprehensive security plan for its DMV offices and driver's license storage and production facilities, databases, and systems utilized for collecting, disseminating or storing information used in the issuance of REAL ID licenses. As part of this requirement, DHS will require that each State include in its annual certification information as to how the State will protect the privacy of the data collected, used, and maintained in connection with REAL ID, including all the source documents.[7]

By requiring states to certify and validate this certification on an annual basis, DHS will hold states strictly accountable for adherence to the highest data security and privacy standards, without dictating specific data security procedures. The required comprehensive security plans and annual recertification updates will give DHS the opportunity to recommend and oversee steps to continuously enhance the security and privacy of state programs as enabling technology evolve and any new threats are identified. For example, best practices can be shared regarding the best means to encrypt customer data during verification checks and to prevent unauthorized access to stored information. This new oversight, guidance on national trends and threats, and sharing of best practices will safeguard the privacy of Americans while also improving security.

Closer collaboration between states and the federal government, together with innovators in the information technology industry, will facilitate the integration of established technology measures that can be applied in a multi-layered approach to further improve security and enhance privacy protection. Examples include:

- Role-based security level systems that limit access to systems and data based on defined roles that can be set at the individual level;
- Enhanced business rules to control what users can do and to prevent corrupt data or incorrect transactions from entering the system;
- Use of data warehouses and reporting tools to look for anomalies that point to fraudulent activity;
- Web-based training and knowledge management tools to give employees better decision information;
- And document scanning and authentication technologies with the ability to authenticate documents such as birth certificates.

Nothing in the REAL ID Act or the NPRM will result in the federal government obtaining more information from driver records than exists today, nor is there additional information about the holders of driver's licenses that the federal government will be able to access or store. This fact is explained in detail in the NPRM, though it is often misinterpreted and misrepresented by many opponents.

From a privacy perspective, the greatest cost to an identity theft victim can occur when a state motor vehicle office, through weak controls or incomplete adjudication, issues a driver's license or identification card to a fraudulent applicant using a stolen Social Security number. There are tens of thousands of instances where identity theft victims have been charged with driving violations, crimes, and tax avoidance because a state has issued a valid identity document on the basis of a stolen Social Security Number, sometimes accompanied by the stolen name of the rightful holder of the Social Security Number. REAL ID will reduce these very harmful invasions of privacy by strengthening the authentication and verification process for issuing driver's licenses. Every step taken to increase security also contributes to privacy protection.

Added Privacy and Data Security Protection

The privacy and security of citizens personal information is one of the most important components of creating a secure identity management system. At the federal level, the

1994 Driver's Privacy Protection Act (DPPA)[8] is the primary law that restricts how driver's license data can be used by states, and that law will continue to apply as REAL ID is implemented. DPPA bars states and their employees from selling or releasing personal information such as Social Security numbers, photographs, addresses, telephone numbers and birthdays, except under limited and legally prescribed circumstances. Should additional privacy protection be needed, the states should work with the federal government to strengthen DPPA to add greater protection of driver's license and identification document data.

DHS' NPRM correctly identifies existing vulnerabilities of data contained on the face of driver's licenses. DHS does not have authority to override state laws which provide open records. Because of the reported data-skimming activities of taverns and other commercial businesses, it would be wise for states to shift toward closed records. Alternatively, states can enact laws to ban retail establishments from capturing data from the face of IDs or from the machine-readable zone on the back of the card. The American Association of Motor Vehicle Administrators (AAMVA) has developed model legislation to prevent the capture and storage of information obtained from a driver's license or identification document. Some states have already barred such activities and have enforced the ban by establishing substantial fines for offenders, and in some cases, removing their liquor or retail licenses.

Conclusion: Real Privacy through REAL ID

Though not originally intended for this purpose, the driver's license has become the most commonly accepted form of identification for many purposes beyond driving motor vehicles. Because of these multifold usages, the driver's license has become the target for theft, counterfeit and falsification by thousands of abusers ranging from terrorists to young teenagers. Given these costs, including the tragic attacks of 9/11, steps must be taken to improve the security and reliability of driver's licenses.

Though printing and communications technologies have aided the abusers of driver's licenses, other proven information technologies are available today to give driver's licenses a new, much-needed level of security and integrity while also safeguarding the privacy of the individuals who make use of them daily.

By creating a minimum level of identity authentication, verification, and card security, REAL ID will improve security and privacy. States will continue to operate and control the state-to-state data exchange process and to verify records with federal databases.

REAL ID introduces no new threat to the privacy of Americans. In fact, its provisions will enhance that privacy, both directly and indirectly, by deterring identity theft and introducing new oversight of systems and procedures to protect personal information collected and stored at the state level. Every step taken to increase security also contributes to privacy protection.

Recommendations of ITAA

1. Congress, the Administration, and the States should fund and implement the REAL ID Act without further delay.

2. Once REAL ID programs are established, the federal government should help states continue to improve security and privacy as part of the annual recertification process. The information technology industry and other representatives from the private sector can contribute much to this on-going effort.

3. To enhance security at the state level, states that have not already done so should pass legislation to prevent the capture and storage of information obtained from a driver's license or other identification document. Such bans should be enforced with substantial penalties.

About ITAA

The Information Technology Association of America (ITAA) provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. ITAA consists of over 325 corporate members throughout the U.S. The Association plays the leading role in issues of IT industry concern including information security, taxes and finance policy, digital intellectual property protection, telecommunications competition, workforce and education, immigration, online privacy and consumer protection, government IT procurement, human resources and e-commerce policy. ITAA members range from the smallest IT start-ups to industry leaders in the Internet, software, IT services, digital content, systems integration, telecommunications, and enterprise solution fields.

ITAA has an active identity management group. Our members include companies producing driver's licenses and other identity cards; managing federal, state and local smart card and identity credentialing programs; providing biometric devices, radio frequency identification technologies and middleware solutions; as well as performing background checks and other identity proofing services.

For more information, visit www.itaa.org. ITAA also serves as secretariat of the World Information Technology and Services Alliance, consisting of 70 IT trade associations around the world.

Footnotes

[1] "Year of First State Driver License Law and First Driver Examination," Table DL-230 (June 1977), U.S. Department of Transportation, Federal Highway Administration, Highway Statistics Summary to 1975, U. S. Government Printing Office, Report No. HWA-HS-S75, p.71

[2] Public Opinion Strategies

[3] Federal Trade Commission, *Consumer Fraud and Identity Theft Complaint Data*, *January – December 2005*, January 2006

[4] Federal Trade Commission, Overview of the Identity Theft Program, Sept 7, 2003

[5] Notice of Proposed Rule Making, 4410-10, Department of Homeland Security, Office of the Secretary, 6 CFR Part 37, Docket No. DHS-2006-0030, RIN 1601-AA37, Minimum Standards for Driver's licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes p. 26

[6] Ibid, p.32

[7] Notice of Proposed Rule Making, 4410-10, Department of Homeland Security, Office of the Secretary, 6 CFR Part 37, Docket No. DHS-2006-0030, RIN 1601-AA37, Minimum Standards for Driver's licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes p. 27

[8] Drivers Privacy Protection Act 18 U.S.C. § 2721 et. seq. (Public Law 103-322)