

Modernizing the State Identification System *An Action Agenda*

By Shane Ham and Robert D. Atkinson

The Sept. 11 hijackings illuminated many holes in our domestic defense. Four of the five hijackers who crashed into the Pentagon, for example, had fraudulent ID cards obtained in Virginia. But the flaws in our identification system were evident long before that. Fake ID cards are so common as to be almost a rite of passage for American teenagers. The industries that rely on the wildly unreliable identification system we have today have watched identity theft grow into a major industry. Worst of all, the ease with which criminals can obtain false identification documents in some states renders the entire system suspect, as possession of a valid driver's license is taken as unquestionable proof of identity for the distribution of other important identity documents—passports, social security cards, employee ID cards, and many more. The Sept. 11 tragedy made vivid the risks inherent in our flawed identification system, but those risks have always been there and we pay for them every day—in higher credit card interest rates to cover for identity fraud, in victimization by criminals who avoid arrest, in suffering and death caused by underage drinkers who get behind the wheel.

Though we have long known that our identification system is broken, we now have a key opportunity to obtain consensus on fixing it. If done properly, a new identification system can not only reduce the threat of terrorism as well as more common crimes, but

also lead to significant economic benefits. Placing 21st-century technology on our driver's licenses and ID cards will jump-start the New Economy, making offline and online transactions more convenient and more secure than ever before.

To accomplish this, there is no need for the federal government to build a new infrastructure for issuing "national ID cards." Modernizing the current system, in which the primary form of identification is issued by the Department of Motor Vehicles in each state, will be sufficient, provided that Congress requires an appropriate amount of standardization both in the cards themselves and in the processes for issuing them.

To do that, action is needed in Congress and in state legislatures. **PPI recommends that Congress:**

- require states to issue "smart ID cards" containing a standardized hologram and digitally encoded biometric data specific to each holder;
- set standards for initial identity verification;
- accelerate the linking of state DMV databases;
- provide grants and loans for additional state smart card applications;

- upgrade the system for foreign visitors to incorporate a similar “smart visa” program; and
- create strict controls to protect privacy and prevent abuses.

States should:

- issue digital signatures with smart ID cards;
- develop and promote other government applications to take advantage of smart ID card capabilities;
- facilitate access to the chip on the card so that card holders could allow private organizations to place applications (e.g., digital cash) on the unused parts of the chip; and
- reduce or eliminate fees for first-time upgrades from old cards to smart cards.

Principles of a Modern ID System

While it is clear that the identification system should be modernized, an undertaking of such importance (and such expense) must be done with a strategic vision in mind. Though the specifics of a modernization plan can be worked out according to costs and available technologies, there are several principles that should be followed when developing legislation.

Maintain the state ID system

Rather than moving to a national identification system in which identification cards are issued by the federal government, modernization should focus on upgrading the current system run by state DMVs. States already have the infrastructure and personnel to issue cards to their citizens. To build a new

federal system would be wasteful.

Maintaining the state system would have important symbolic value as well. Many Americans worry that federal consolidation of all identity information could be detrimental to privacy and liberty. Though the federal government is no more likely to abuse this information than state governments, there is no compelling reason to engage in such an argument when the states are capable of upgrading their own systems. The federal government, on the other hand, should modernize its visa system to incorporate smart visas with biometric identifiers.

Focus on the integrity of the system

The integrity of the identification system rests on the validity of the initial identity verification. If someone can get a state-issued ID card using a fake document (such as a forged birth certificate) or an untruthful affidavit (as happened in the Virginia ID fraud ring), the rest of the system is corrupted. This is especially true because many other forms of identification are issued based solely on the possession of a valid state driver’s license or ID card. Once a single false identity is obtained, it is easy to obtain false passports, false bank accounts, or false state-issued ID cards in other states. To ensure that the identification system works, the focus of state DMVs granting an initial card must be on verification rather than customer convenience.

Similarly, it should be impossible to get more than one ID card at a time. State DMVs already require that drivers surrender any current license from a different state before being granted a new one, but drivers are not always forthcoming about being a current license holder (particularly if the driver has a suspended license). More significantly, many holders of driver’s licenses or visitor visas get second cards under a false identity (either for purchasing alcohol while under age or to commit fraud). To prevent this, and to reduce the costs of performing the initial identity

verifications, a modernized identification system must be able to detect individuals who seek a new card while secretly holding another.

Improve the integrity of the card

Many criminals do not even need to defraud the DMV to get a fake card. The widespread availability and low cost of sophisticated graphic software and high-quality color printers have made fake identification cards easier than ever to generate. Templates for fake ID cards can be downloaded from the Internet, and many Web sites offer to create fake ID cards for a fee.

Many states use holograms or other security features that are difficult to reproduce, but bank tellers or airline agents may not know which ID cards should have holograms on them. Moreover, visual security features often become useless as the result of an anti-fraud “arms race” between criminals and state governments. (The same arms race requires the occasional redesign of currency to battle counterfeiters.) Efforts to update state ID cards must therefore also aim to bring the latest technology to bear on more effective visual and electronic markers for verifying authenticity.

The Congressional Agenda

Though the identification system will continue to be managed by the states, Congress has an important role in setting minimal standards to ensure the system’s security and integrity. The need to establish secure identity cards is so compelling, and the economic benefits so large, we believe federal intervention—in the form of both mandates and incentives—into an area traditionally considered a state prerogative is required.

Require states to issue smart ID cards

Smart cards are simply cards implanted with small computer chips that can hold data and perform other functions.¹ In addition to the biometric data written on the card (photographs and height, weight, and eye color data), the chips would hold an encrypted version of a unique biometric identifier, such as a digital scan of a thumbprint. In situations where additional verification of identity is needed, such as traffic stops or airport security gates, the card holder could simply place his thumb on an inexpensive scanner, and by comparing the scan against the data in the smart card, the scanner could verify both that the card is legitimate, and that the presenter of the card is its rightful owner. Because the digital biometric data is both unique and encrypted, it would be virtually impossible to create a fake ID card or to use someone else’s ID card.

Because the identification data takes only a small portion of the chip, and because the chip can be partitioned into many segments with secure firewalls, smart cards can be used for a host of other applications, including digital government. States that issue smart ID cards can also use them for other functions such as Electronic Benefits Transfer (e.g., digital food stamps), voter registration, library cards, hunting and fishing licenses, and many others. Smart ID cards will also enable more secure online transactions, as verifying identity and “signing” documents online will be a simple matter of placing the smart card (and a thumbprint) on an inexpensive reader that attaches to a home computer.² Smart ID cards could also be used to create a frequent flyer “fast lane” that enables trusted individuals to skip some of the security requirements at airports.³ If they wanted to, individual cardholders could also let private companies use space on the cards for applications ranging

from digital cash to downloadable hotel room keys. These and other mobile e-commerce applications would significantly boost consumer convenience and economic productivity. By resolving the “chicken or egg” dilemma facing the widespread adoption of smart cards, and by reducing identity theft, the modernized identification system would give a major boost to the economy.

Many states have either already modified their ID cards or are in the process of doing so, using so-called “2D bar code” technology. Unlike the series of thick and thin vertical bars used in Universal Product Code symbols, these fuzzy images can encode enough information to store both the information written on the front of the card and a mathematical representation of biometric data. Other states are using magnetic stripes on their ID cards, similar to the stripes on credit cards. While these innovations do make the cards “machine readable,” they are considerably less secure; a 2D bar code, for instance, can be created on a home printer and laminated to a driver’s license. Once hackers determine the encryption scheme for the bar codes, the entire system is corrupted; smart cards carry individual encryption, so in the unlikely event that one card is hacked, the rest of the cards remain secure. 2D bar codes also fail to take advantage of the significant economic benefits that can be derived from putting a smart card in the pocket of nearly every American. As such, these lesser technologies are a poor investment; they do not deliver the same bang for the taxpayer’s dollar.

Unfortunately, most state DMVs have shown little enthusiasm for smart cards, for operational, financial, and political reasons.⁴ **Congress should require that all state-issued ID cards contain smart chips configured to be used by the government but also to allow individuals to let private companies put applications on the card.** The cards could continue to be “backward compatible” with other existing ID card technologies, by

retaining magnetic stripes or printed bar codes in addition to the chip. To speed the process of adopting smart ID cards, **Congress should also provide funding for a standards-setting committee, consisting of government and industry representatives and organized through the American Association of Motor Vehicle Administrators (AAMVA), to set standards on smart ID card interoperability as quickly as possible.**

Require digitally encoded biometric data specific to each user

Of all the proposals to modernize the identification system, none is more controversial than adding biometric data such as thumbprints or iris scans. The controversy, however, has less to do with facts than it does with the inflammatory statements of civil libertarians and privacy advocates who present biometrics as a quantum leap forward in high-tech surveillance.⁵ In fact, every state-issued driver’s license and ID card already contains a wealth of biometric data on sex, age, height, weight, hair color, and eye color, as well as a photograph. The validity of the ID card is proven when a person matches this information to the cardholder. **Adding a digitized thumbprint or other biometric data to an ID card does not add a privacy violation or even change the fundamental principle underlying the ID card: to compare data on the card with the body of the person presenting the card.**

Seen this way, adding digitized biometric data is merely a needed improvement that technology enables. Encrypted data on a smart chip is much harder to forge than an image of a driver’s license. Thumbprints and iris scans are unique to an individual, unlike the vague information on the front of an ID card. (Even photographs are not foolproof, as criminals can claim that the photograph on a stolen ID card was taken before they gained weight, or some similar excuse.) Most importantly, digitized biometric data does not need to be

viewed by human eyes; during an online transaction a remote computer can verify that its rightful owner is using the card in the reader.

Privacy advocates also worry about the expansion of government power that might result from requiring every citizen who wants a driver's license or ID card to surrender a thumbprint. Currently police gather such information only when a person is arrested for a crime. (A conviction is not necessary to make fingerprints part of the permanent database.) Because the biometric data would need to be held in a database to confirm the identity of individuals who claim to have lost their ID cards, there is a fear that the DMV thumbprint database could eventually be used to solve crimes, even if that use is specifically prohibited when the database is first created.

This dilemma can be solved by the collection of two different biometric measures. A thumbprint could be encoded on the card but not kept in a central database. This allows anyone with an inexpensive handheld scanner to verify that the individual presenting the card is the same individual to whom the card was issued.⁶ For purposes of maintaining a biometric database for preventing multiple ID cards or ID switching, iris scans or other ephemeral biometric data could be used.⁷ Using ephemeral biometrics for the database ensures that the data could never be used for law enforcement, since (unlike thumbprints) images of the iris are never left behind at crime scenes. **Congress should therefore mandate that states implement a dual-track biometric data collection process, with thumbprints carried onboard the smart ID cards and ephemeral biometrics archived in a database to verify the identities of all individuals who have previously been issued an ID card.**

Require a standardized hologram on the card

Because states are free to design their driver's licenses and ID cards, it is often

difficult for a grocery store cashier or bank teller in one state to determine if an ID card from another state is legitimate. Does Montana still issue laminated cards? Is the Iowa card supposed to have a holographic overlay or not? Did New Hampshire recently redesign its cards? These questions could be resolved with a standardized anti-fraud feature.

The most obvious candidate for standardization is a hologram. Each state could continue to design its own cards, but would overlay them with a hologram that is the same in every state. Anyone wishing to verify that the card was issued by a state DMV—as opposed to an Internet fraud artist—would only have to hold the card to the light. (Holograms are notoriously difficult and expensive to reproduce, making it impossible to create a fake ID on a home computer.) Congress should direct the Department of Transportation to select an image for the standardized hologram (such as an eagle or the American flag) and require all state-issued ID cards to display the hologram.⁸

Set standards for initial identity verification

A state-issued ID card is usually considered sufficient for proving identity; in fact, most states will issue a driver's license or ID card when presented with a card from another state. Implicit in that policy is the assumption that the first state to issue an ID card verified the true identity of the holder. Unfortunately, that's far from the truth. It is relatively easy to get an ID card under a false identity by creating a false birth certificate or ordering a copy of another person's birth certificate. Some states also accept signed affidavits from various parties as proof of identification.

The states have undertaken some efforts to tighten up their systems. One program is the Social Security Online Verification (SSOLV) program, which allows state DMVs to check an applicant's Social Security number against

the Social Security Administration's database in real time.⁹ This is useful, but not all applicants are willing to submit their Social Security number to a state agent. Moreover, not all states participate in the program.

Congress should therefore set minimum standards for documentation that states must require before issuing an ID card. The standards should not only specify which documents are acceptable (such as birth certificates, passports, immigration documents, and so on), but also require states to verify their authenticity by checking with the agency that issued the documents.¹⁰ Proof-of-residency requirements should also be stricter, involving more than presentation of a utility bill.¹¹

Accelerate the linking of state DMV databases

Though state motor vehicle agencies do engage in limited information exchange (typically on bad drivers), it is still relatively easy to get ID cards under multiple identities in different states. Though efforts have been undertaken to ensure that drivers with suspended licenses cannot get new licenses by traveling to another state,¹² the requirements are not as strict for ID cards or for drivers who have not lost their privileges but claim falsely that they have never been issued a license in another state.¹³ The key to preventing the issuance of multiple ID cards is linking the full databases of all state DMVs. This would virtually eliminate the practice of ID switching, and if tied in with a smart visa proposal, would prevent foreign visitors from obtaining driver's licenses and then hiding out in the United States after the visas expire.

The 1998 highway bill¹⁴ made a small appropriation for a feasibility study on linking the databases, a study which is still ongoing. The integration process must be greatly accelerated. To that end, **Congress should appropriate funds to facilitate integration of state DMV databases.** The appropriation

should be contingent upon the state DMVs' agreeing to capture ephemeral biometric data for storage in their databases, to ensure that no individual can claim first-time applicant status after being granted a card in another state.

Provide grants and loans for additional state smart card applications

Resistance by state governments to modernizing ID cards with smart chips will diminish when states realize that they are able to use the cards to make their own government operations more efficient. From the electronic food stamps that most states have implemented, to the secure voter registration that is a key to election reform, to the secure online transactions that will reduce the lines in various state offices, states have a multitude of uses for the "spare" space on smart cards. Given that citizens have more contact with state and local governments than they do with the federal government, a card that makes those contacts easier will be widely embraced. Moreover, the increased efficiency will show on the bottom line of state budgets.

Unfortunately, because many states are experiencing serious budget crunches, it will be difficult to find the funds to run pilot projects for smart card applications. **To encourage states to make innovative use of smart cards, Congress should provide matching grants to states that initiate pilot projects. As other states decide to adopt the systems developed in successful projects, Congress should make matching grants to speed deployment.** Such investments in smart card infrastructure will guarantee the best leverage of the modernized ID system.

Upgrade the system for foreign visitors to a "smart visa" program

An ID system for U.S. citizens would not be very effective for domestic defense if the system did not also apply to foreign visitors. The biometric smart card system proposed for

driver's licenses should therefore be extended to anyone wishing to enter the United States legally. (Ideally, Canada would develop a similar interoperable system.) The current visa program should be upgraded to issue visas as smart cards with biometric data. Those countries that wish to participate in the visa waiver program—so their citizens can enter the United States without obtaining a visa – would be required to issue smart passports with biometric data.¹⁵

Just as with the ID system, smart visas are only as effective as the initial identity verification. The U.S. embassies that issue the visas must become the first line of defense in keeping potential terrorists out of the country. Access to data regarding suspected terrorists is an important part of that defense, but it may become necessary to impose stricter criteria for granting visas to enter the United States. If an individual seeking to visit the United States cannot prove beyond a doubt his or her identity and good standing, a visa should not be granted. Along those same lines, the U.S. government needs to take a closer look at the countries that participate in the visa waiver program to ensure that they are taking sufficient steps to combat ID fraud.

In the aftermath of the terrorist attacks, Sens. Edward Kennedy (D-Mass.), Dianne Feinstein (D-Calif.), and Jon Kyl (R-Ariz.), among others, sponsored bipartisan legislation (S. 1749) to improve the visa system. The legislation calls for the deployment of smart visas with biometric scanners at each point of entry by late 2003. **Congress should act expeditiously to pass the smart visa bill.**

Create strict controls to protect privacy and prevent abuses

Though much of the rhetoric privacy advocates use against smart ID cards is exaggerated, there are legitimate privacy concerns that need to be addressed. As we pointed out in *Frequently Asked Questions About Smart ID Cards*,¹⁶ these concerns don't

arise from the smart ID cards themselves. The technology is privacy-neutral; it is the rules that govern the technology that should concern us. Congress should therefore legislate controls over the use of smart ID cards, including:

- mandate that the “onboard” thumbprint scans only be used to match the card to the card holder, and never be stored in a central database;
- prohibit state DMVs and other government agencies from selling any information—government or private—stored on the card;
- specify that the rules that govern the circumstances under which an ID card must be presented and the information recorded by government agents will not change with the addition of computer chips to the cards;
- prohibit private companies from using the “official” data on the cards for any purpose other than verifying identity (e.g., grocery stores may not capture age and gender data to ascertain shopping habits);
- specify that verifying the card against the onboard biometric data will be optional in non-secure facilities (e.g., airports may be required to check the thumbprint scan but bartenders will not); and
- impose severe criminal penalties on anyone who attempts to “hack” a smart ID card, and attach substantial liability to manufacturers that sell cards with serious security defects.

The State Agenda

Issue digital signatures with smart ID cards

There was much fanfare in June 2000 when President Clinton signed the “E-Sign” bill,

which made digital signatures legally binding on all documents. The legislation was meant to herald a new era of efficiency, in which documents could be signed over the Internet, saving hundreds of millions of dollars every year. Unfortunately, the promise of the E-Sign bill has not come to fruition, primarily because of the chicken/egg issue: Nobody accepts digital signatures because nobody has secure digital signatures tied to their true identity.

Smart ID cards could resolve this problem. Digital signatures issued in conjunction with a state driver's license or ID card would have a tremendous advantage over current signatures. Most obviously, a certificate issued by the state and stored on a smart card would have the benefit of the identity verification conducted by the state DMV. By issuing a digital signature to every card holder who requests it, applications for digital signatures would move beyond the business-to-business world and into more ordinary transactions that require valid signatures, from real estate closings to living wills to online bank accounts. **States should offer citizens the opportunity to place an encrypted digital signature on their smart ID cards at the time of issuance.**

Develop and promote other government applications to take advantage of smart ID card capabilities

Taking advantage of smart ID cards to streamline government processes will give the greatest return on the initial investment to modernize the identification system. Increased protection from both terrorists and criminals is an important goal (with implications for the bottom line in state and local budgets), but it is also important to take full advantage of the technology's potential. The next generation of digital government applications—particularly on-line transactions that require secure verification of identity—can be boosted by

the distribution of smart ID cards.

Whether or not Congress provides funding to get new smart card applications off the ground, state and local governments would be wise to invest in new smart card applications to streamline government interaction. Among the possible applications:

- hand-held devices for police officers that can read and verify smart ID cards, putting an end to writing down driver's license information on paper citations;¹⁷
- upgraded Electronic Benefits Transfer system to reduce food stamp fraud with biometric verification;
- voter registration and identification, including an interlinked voter sign-in database to eliminate the possibility that the same individual will vote in multiple precincts (which in turn will eliminate the need for early voter registration), as well as secure online voting;
- integrated digital cash systems, to allow one card to pay for parking meters, highway tolls, public transit, and so on;
- online adjudication of minor violations such as traffic citations.
- paying taxes; and
- obtaining or renewing licenses and registrations.

Of course, this is not a comprehensive list of all possible digital government initiatives that can take advantage of smart cards. State and local governments should look carefully at all of their processes and procedures in which smart cards can either streamline the collection of data that might otherwise have to be written on paper and then entered into computers by hand, or can eliminate the need for citizens to present themselves in person for a visual verification of their identity or for a legally binding signature.

Facilitate access to the chip on the card so that cardholders can allow private organizations to place applications on the unused parts of the chip

Not all of the economic benefits of smart ID cards come from streamlined government operations; many come from the private sector. Smart cards are already in use for a number of applications, from the SpeedPass key fobs at gas stations to key cards on office buildings. Still, many companies are reluctant to use smart cards because a card with only one use has wasted capacity, and therefore wasted expense. The number of smart card applications will explode, however, when DMVs begin issuing smart cards with an open architecture. **With virtually every adult in the nation carrying a smart card, companies will not have to invest in their own chip cards or fobs to take advantage of smart card applications.**

This creates a tremendous funding opportunity to pay for the cards. Private firms will gladly pay for the privilege of downloading their applets onto their customers' smart ID cards, since it will save them the expense of manufacturing and mailing their own card. If every cardholder transferred just two or three functions to their driver's license—an ATM card, a credit card, a garage access key, a frequent flyer number, a grocery store discount card—the improved cards could pay for themselves. Through the use of encryption and firewalls, these different applications can safely coexist on a single card with no risk of one entity seeing the data left on the card by another.

It is important, however, that control over the “free space” on a smart ID card be left to individual cardholders. While state governments should place other government applets onto the cards, they should not allow companies to install applets on every card issued for a flat fee. Individuals must be allowed to decide which private firms they

trust enough to place applications on their cards. States should only collect revenue from companies after the cardholder has made the decision to download an applet to the card on and should charge the companies on a “per download” basis.

Taking advantage of this opportunity, therefore, will require coordination between the states. Since access fees on the card will be paid on a per-customer basis, companies that want to download applets to customers across the nation will need a centralized system for paying the fees. States should work together through AAMVA to develop such a portal to facilitate the revenue stream that will make the modernization of the identification system more affordable.

Reduce or eliminate fees for first-time upgrades from old cards to smart cards

A driver's license or ID card is typically good for four or five years, but the renewal fee is paid up front rather than spread out over that time. Getting a new driver's license and paying another fee before the expiration date, therefore, constitutes an additional tax. Despite the benefits of having a smart card, people may be reluctant to upgrade their current ID to a smart ID card before they are forced to do so by the expiration date, particularly if smart card fees rise considerably.

To get the quickest benefits from improved security and the network effects of distributing the smart cards, state DMVs should offer incentives for upgrading the current cards before the expiration date. The best way to do so, obviously, would be to offer a free upgrade, in effect restarting the clock on the renewal fee.¹⁸ If budgetary constraints make that impractical, the fees should at least be prorated. For instance, if state law requires renewal of a driver's license or ID card every four years, and someone's card expires in two years, that person should be able to upgrade to the smart card at a 50 percent discount.

Conclusion

Modernizing the identification system will require more than investment in hardware and software; it will also require considerable political courage and will. A small but vocal fringe of special interest civil liberty and privacy groups has already begun to demagogue the issue in the media. Countering such misinformation and paranoid scenarios about “tracking” the movements of citizens will take a patient and concerted education effort.

Once in place, however, smart ID cards will improve our security while helping transform government operations and boost economic productivity. Given the need to modernize the system for domestic defense purposes, it would be unwise to take partial steps forward with second-rate technology, particularly since undertaking a less effective modernization effort will do nothing to quell the irrational core of critics. Transforming the identification system is something that must be done—we should do it right the first time.

Shane Ham is the senior technology policy analyst at the Progressive Policy Institute, and Robert D. Atkinson is vice president and director of PPI's Technology & New Economy Project.

For further information about PPI publications, please call 800-546-0027, write the Progressive Policy Institute, 600 Pennsylvania Ave., Suite 400, Washington, DC, 20003, or visit PPI's web site at: <http://www.ppionline.org>.

Endnotes

- ¹ Some smart chips are mere memory chips designed to store data, whereas more sophisticated cards are actually miniature computers, with operating systems, RAM and ROM sectors, and encryption coprocessors. These more sophisticated chips are what we mean when we say “smart cards.”
- ² Smart card readers and thumbprint scanners are available now and are inexpensive, but most computers are not sold with such devices because there are so few smart cards in use. If, however, every driver’s license and state-issued ID card were converted to a smart card, such equipment would quickly become standard on every new computer sold.
- ³ For more on the use of technology for airport security, see “How Technology Can Help Make Air Travel Safe Again,” by Robert D. Atkinson, at www.ppionline.org.
- ⁴ A 1999 report by AAMVA on smart cards, citing concerns from security to durability, concludes that there is “no strong business case for the use of smart cards in either driver licensing or vehicle registration applications at this time.” <http://www.aamva.org/Documents/stdSmartCardFinal.pdf>
- ⁵ For a comprehensive response to the issues raised by privacy advocates with regard to smart ID cards, see “Frequently Asked Questions About Smart ID Cards,” by Shane Ham and Robert D. Atkinson, at www.ppionline.org.
- ⁶ For more information about the importance of handheld scanners for domestic defense, see “Using Technology to Detect and Prevent Terrorism,” by Shane Ham and Robert D. Atkinson, at www.ppionline.org.
- ⁷ There are other potential candidates for a biometric verification database, including hand geometry, facial geometry, or even digital photographs. The important point, from a privacy perspective, is that the information stored in the database is ephemeral, and could not be left behind at a crime scene as a thumbprint or DNA sample might.
- ⁸ Holograms are the best technology currently available, but it is entirely possible that fraud artists will be able to create inexpensive fake holograms in the future. Just as with the design of our currency, the federal government must be alert to the ongoing “arms race” with criminals, and be prepared to upgrade the standardized security feature.
- ⁹ The system does not allow DMV agents to see any information except the name, date of birth, and Social Security number of the applicant. For more information, see http://www.aamva.org/drivers/drv_AutomatedSystemsSSOLV.asp.
- ¹⁰ This is a relatively easy task for citizens born in the United States, though the process may take several days. Many states are beginning to place vital statistics online, and check birth records against death records, which can make the process even faster. Foreign citizens may not be so lucky, so the federal government must verify their entry documents. More stringent verification of the identity of immigrants and foreign visitors is an important part of domestic defense, and should be undertaken by the federal government irrespective of the effort to modernize the identification system in the United States.
- ¹¹ Residency can be checked by accessing online property records, placing a phone call to landlords, or by checking address records in private databases such as those compiled by credit reporting bureaus.

¹² The National Driver Registry, a database of all drivers whose privileges have been suspended, is maintained by the National Highway Transportation Safety Administration.
<http://www.nhtsa.dot.gov/people/perform/driver/>.

¹³ An interstate compact mandates that states require all applicants who claim to have no prior driver's license or ID card issued in another state to submit a notarized statement to that effect. However, there is no method for verifying the truth of such statements.

¹⁴ Transportation Equity Act for the 21st Century (TEA-21), P.L. 105-178.

¹⁵ Under a bipartisan compromise bill on visa reform introduced in the Senate (S. 1749), visa waiver countries would only have to report stolen passports, not require biometric identification.

¹⁶ www.ppionline.org.

¹⁷ The handheld devices should also be used to access any databases that the officers might check as part of a routine traffic stop. For more detail on the handheld device proposal, see tech terrorism paper referenced in note 6.

¹⁸ Free upgrades could be cut off for cards that are approaching the expiration date; for instance, upgrades could be free only for cards that are still good for six months or more.