

# Technological Innovation Without Big Brother

## *Privacy Principles for Government in the Information Age*

*By Shane Ham and Robert D. Atkinson*

In the wake of the September 11th terrorist attacks, increased airline security became a nightmare for passengers. The long lines at checkpoints have since shortened, but the system for selecting passengers for the most thorough screenings remains a major irritant to travelers. In response to the need for tight, yet efficient, airline security, the Transportation Security Agency (TSA) set out to develop a new Computer Assisted Passenger Prescreening System (CAPPS II) designed to automatically identify passengers who are high-risk while letting “trusted” travelers through to the gates with only the normal screening process. But throughout the process of developing CAPPS II, privacy advocates protested. The American Civil Liberties Union, for example, issued a press release calling CAPPS II “a secretive new system for conducting background checks on all airline passengers,” and warning that the system threatened to create “a bureaucratic machine for destroying Americans’ privacy and a government blacklist that will harm innocent Americans.”<sup>1</sup> In large part because of protests like this, the Bush administration announced in July that it was scrapping plans for CAPPS II.

This is but one of many examples of how concerns over privacy are slowing government use of new information technologies that promise to streamline public sector operations, increase productivity, improve service quality, and boost mission effectiveness. It is a trend that has important consequences because the public sector lags far behind the private sector in taking advantage of

information technology (IT), even for practical applications unrelated to homeland security. Examples of those applications range from electronic tollbooths that can help keep traffic moving to websites that can offer 24-hour access to government services. The benefits that such innovations offer should be seen as welcome developments for citizens and taxpayers.<sup>2</sup> They are emblematic of the sort

***“One person with a belief is a social power equal to ninety-nine who have only interests.”***

**—John Stuart Mill**

## **The Progressive Policy Institute**

The Progressive Policy Institute is a catalyst for political change and renewal. Its mission is to modernize progressive politics and governance for the 21st century. Moving beyond the left-right debates of the last century, PPI is a prolific source of the Third Way thinking that is reshaping politics both in the United States and around the world.

PPI invents new ways to advance enduring progressive principles: equal opportunity, mutual responsibility, civic enterprise, public sector reform, national strength, and collective security. Its “progressive market strategy” embraces economic innovation, fiscal discipline, and open markets, while also equipping working families with new tools for success. Its signature policy blueprints include national service, community policing, and a social compact that requires and rewards work; new public schools based on accountability, choice, and customization; a networked government that uses information technology to break down bureaucratic barriers; pollution trading markets and other steps toward a clean energy economy; a citizen-centered approach to universal health care and a progressive internationalism that commits America’s strength to the defense of liberal democracy.

Rejecting tired dogmas, PPI brings a spirit of radical pragmatism and experimentation to the challenge of restoring our collective problem-solving capacities—and thereby reviving public confidence in what progressive governance can accomplish.

*The Progressive Policy Institute is a project of the Third Way Foundation.*

[www.ppionline.org](http://www.ppionline.org)



of digital transformation that should be encouraged in the public sector.

It is certainly true that the loss of privacy is an increasingly common fear in the digital age. It can sometimes seem that we are being spied upon during every waking moment: There are security cameras at the convenience store where we get our coffee in the morning and “cookies” tracking our web surfing habits when we’re at home in the evening. Government invasions of privacy are a potentially greater threat than those presented by businesses, because unlike advertisers and other private entities that collect information about us, government has the power to strip us of our property and our freedom. Particularly under the current administration, which has suggested in writing that some laws may not apply to the president dur-

ing the war on terrorism, fear of the government is becoming less the province of the paranoid and more of a common thread in modern life.

But privacy fears are easily blown out of reasonable proportion. There are influential advocacy groups that regularly mount well organized and often misleading campaigns in the press, online, and in public hearings, against entirely appropriate government technology initiatives. Several case studies are detailed in this report, from resistance against red light cameras as “Orwellian,” to protests against upgraded databases at state motor vehicle agencies. The most strident privacy advocates argue that potential harms to citizen privacy from such initiatives far outweigh the potential benefits.

The Progressive Policy Institute takes the opposite view. We believe that with the right rules and safeguards in place, government can increase its use of advanced information technology tools and realize significant benefits for society as a whole without causing unacceptable harms to the privacy of citizens. The PPI further believes that keeping government institutions mired in 20th century operating methods while the rest of the global economy advances is not an option.

The United States today is in a transition period: We are becoming a more digital society. In this transition period, it is essential that we properly balance privacy concerns with the societal interest in unleashing the benefits of new technologies.

## The Need for Privacy Principles

It is important to realize that information technology itself is privacy-neutral; it can be used to enhance or destroy privacy. What matters are the intentions of the technology users and the rules and procedures established to prevent and rectify abuses. Putting in place the right rules and safeguards before new technology systems are up and running can ensure that citizen privacy is protected and abuses are prevented. Moreover, standardizing those protections in all government initiatives would go a long way toward assuring Americans that new technology systems will be used in the best interests of society as a whole, not to make people's lives less private.

Yet, regardless of how extensive the rules and safeguards are, there are some privacy and civil liberties advocates who routinely invoke the image of "big brother" and try to rally opposition to government's embrace of information technologies. The Bush administration has been far too generous in providing these groups with ammunition. The administration has not made serious efforts to develop clear, transparent rules and procedures governing how information is

going to be used. That failure fuels suspicions of the administration's already authoritarian reputation, provides ammunition for privacy advocates, and makes it more difficult for government to take needed steps to modernize its operations.

It is long past time for the administration, Congress, and the states to develop a framework of principles for protecting citizen privacy that can guide the development and deployment

of technology tools by government. The PPI has long advocated the concept of privacy as a balance between individual and societal interests. If that balance is considered in advance, and new technology initiatives are specifically designed to adhere to appropriate privacy considerations, there is no reason that the use of technology tools by government should cause an unacceptable loss of citizens' privacy.

To that end, we propose the following specific principles to guide the use of information technology by federal, state, and local governments. These principles are particularly relevant in cases where new technologies are most urgently needed, such as in law enforcement and homeland security:

1. Rather than barring new technology, we should put in place and enforce clear rules to protect privacy.
2. Data mining can be a powerful tool for fighting crime and terrorism, but needs stringent safeguards.

---

***"It is long past time for the administration, Congress, and the states to develop a framework of principles for protecting citizen privacy that can guide the development and deployment of technology tools by government."***

---

3. Government data requires more rigorous privacy protection than privately held data.
4. Government deployment of new technology must be as transparent as possible to allow for accountability.

## Privacy: A Uniquely Modern Concept

Perhaps the ultimate irony in the controversy over modern technology's role in affecting privacy is that modern technology created privacy. For much of our history, most Americans lived in small communities where privacy was rare and anonymity was practically unheard of. Even today, in many small communities across the country, it is common for everyone to know a great deal of personal information about their neighbors; indeed, many evolutionary psychologists believe that the urge to gossip is hard-wired

in the human psyche.<sup>3</sup> Before the rise of population mobility and mass consumerism, the concept of privacy was largely a matter of good manners—pretending that nobody knew about the health or finan-

---

***“The sheer power of modern information technology tools demands a thoughtful assessment not only of the rules governing the use of IT, but of our beliefs about what privacy should be in the 21st century.”***

---

cial problems of their neighbors.

As anonymity grew, so did the advantages and desirability of privacy, but it came at a cost. It became necessary for people to carry government-issued identification (i.e., a driver's license) as a matter of course. Wider markets and increasing mobility made it necessary for merchants and banks to collect and share data to determine which individuals were bad credit risks. These local and regional credit reporting

bureaus harnessed information technology to trade information on a wider basis, and an industry that barely existed before World War II was national by the 1970s.<sup>4</sup> The difficulty of keeping track of criminals as they crossed jurisdictions pushed the Federal Bureau of Investigation (FBI) to create a national database of wanted criminals in 1967—the National Crime Information Center (NCIC)—a system that has grown into a massive and regularly used database today.<sup>5</sup> The means by which many government databases now identify individuals—the Social Security number—originally came from the need to develop a government retirement insurance system, which required that each citizen be issued a unique number to identify them for benefits purposes.

It is not the case, then, that information technology represents a new intrusion into a long-standing (if not intrinsic) human right; even the Bill of Rights treats privacy as a tradeoff, stipulating that privacy can be violated by the government with due process. Rather, technology has generally been applied to mitigate the side effects of ever-increasing anonymity and make it more difficult for people to switch identities to escape criminal records or commit fraud. Privacy as we know it today—a right to anonymity—is a relatively recent entry onto the scene of American civic values.<sup>6</sup> Nevertheless, it has become an important civic value, and one that must be balanced with other societal needs (for example, national security and economic efficiency) when considering how information technology is to be used by government or by private institutions and individuals.

To be sure, the rise of the Internet has reduced the general level of anonymity and privacy even more quickly than the values of anonymity and privacy took root in the culture. That is not always a bad thing. For example, it has become increasingly common for people to “Google” their friends and dates—that is, to run Internet searches to make sure they are not hiding something important. (Recently a

woman used the Google Internet search engine to determine that her blind date was a fugitive, and turned him in to authorities.<sup>7</sup>) The sheer power of modern information technology tools demands a thoughtful assessment not only of the rules governing the use of IT, but of our beliefs about what privacy should be in the 21st century. Only such an assessment can ensure that government can go forward with technological transformation in the right way.

There are a host of new tools that governments seek to use that have privacy implications. Digitized identification cards can now hold biometric data such as fingerprints in addition to photographs. Remote and Internet-based government transactions require secure ways to verify identity online and securely transmit sensitive data. Automated traffic control systems, such as tollbooths and red light cameras, can potentially track citizen movement if implemented without appropriate privacy rules in place. The federal government seeks the ability to “mine” both public and private data in the hopes of “connecting the dots” that can prevent another major terrorist attack. Meanwhile, countless other examples of a more mundane variety can help streamline government operations. These types of systems can be either helpful or harmful to privacy, which is why they should be developed with a set of principles in mind that respects privacy and recognizes the need for tradeoffs when efficiency or security demands outweigh the privacy interest.

## **Privacy Principles for Government in the Information Age**

Given the wide variety of functions performed by governments and the wide variety of technologies available to help perform those functions, there can be no hard and fast rules for government technology and privacy. Each technology tool will need to be evaluated be-

fore being put into use to determine the appropriate tradeoff between the likely benefits and potential privacy harms, and to determine whether such a tradeoff is even necessary. However, there are some principles that should be followed whenever government is considering a new information technology tool:

### ***1. Rather than barring new technologies as a preventative measure, we should put in place and enforce clear rules to protect privacy.***

Governments at all levels routinely collect and store large amounts of data on every citizen for important and useful purposes. Similarly, governments at all levels engage in routine law enforcement activities that nearly everyone, including ardent civil libertarians, understands to be necessary and appropriate. While some government functions are deviations from an ideal of pure privacy—such as taking the fingerprints of people who have been arrested, but not convicted of anything—these practices are a fair and reasonable tradeoff by individuals for the benefit of society as a whole.

With the explosion of powerful and inexpensive information technology, it is both understandable and desirable that government should try to use technology tools to perform these widely accepted functions more efficiently and less expensively. Some privacy advocates, however, believe that the mere act of upgrading technology to perform an acceptable function is, *per se*, a privacy violation. The Progressive Policy Institute believes that if having armed police officers on the streets observing people is acceptable, then using security cameras to do the same thing at a lower cost is not a privacy violation. If maintaining certain records about citizens on paper forms is fine, then maintaining exactly the same information in a computer database to make record retrieval less costly to law enforcement does not constitute a privacy violation. If keeping fingerprints on paper cards is accept-

able, then storing them in a database that is more easily searched by law enforcement is not a privacy violation. And if keeping data in databases is okay, then with the appropriate safeguards in place it should be okay to have the databases connected to maximize efficiency. But privacy advocates often disagree with that logic. Their view was demonstrated when the Electronic Privacy Information Center (EPIC) released a report criticizing efforts to modernize the state driver's license system. "New technologies can reduce the risk of counterfeiting and fraud," the report found. Nonetheless, the report opposed efforts "to expand the information sharing capacity of DMVs."<sup>8</sup>

It makes no sense to insist that government do its job with outmoded, inefficient, and less-effective technology. The extreme expense of the nation's beefed-up homeland security efforts have drawn attention to this paradox, but the issue existed before the September 11th terrorist attacks. Then and now, transforming government operations with technology tools is not merely a good idea, it is a moral imperative; taxpayers deserve the best government they can get for the least amount of money—and technology tools can save billions of taxpayer dollars.

Of course, that does not mean that information technology could not be abused or deployed in a manner that does in fact harm privacy. Computers, cameras, biometric scanners, and other technologies are powerful tools, and can be abused by government agents or anyone who possesses them. But so too can older technological innovations that government deployed to do its job more efficiently. For example, when police started carrying handguns or driving vehicles, the potential for abuse—with fatal results—was certainly present. Yet society recognizes that the benefits of an armed, mobile police force far outweighed the potential for abuse, and we put in place rules to prevent it. (There are rules, for example, dictating the circumstances in which police can use firearms.)

Despite the potential for abuse, technology itself is privacy-neutral; it is the rules governing the use of technology that preserve or destroy privacy. When a new database or other tool is used by a government agency, it must have rules in place to ensure that it simply streamlines acceptable government functions, and is not used in new ways that have not been contemplated or authorized by the relevant legislative or regulatory body.

***2. Data mining can be a powerful tool for fighting crime and terrorism, but it needs stringent safeguards so that it is not used for unwarranted "fishing expeditions."***

Many complaints regarding potential privacy violations by the government are caused by a conflation of two distinct scenarios: the government learning about an individual during the course of an investigation, and the government "tracking" the ongoing activities of an individual. The latter scenario is what the dystopian big brother government did in George Orwell's classic novel *1984*, and Americans are right to oppose that type of authoritarianism. But the mere availability of information to government agencies does not mean America is a surveillance state.

The reality is that a tremendous amount of information from a staggering array of public and private sources is available about all Americans. From credit card purchase records to addresses for Internet access accounts, to electronic debits on toll booth speed passes, it is possible for an investigator with enough authority and enough manpower to reconstruct many of a given individual's movements. This can be vitally important when building a case against a suspected criminal.<sup>9</sup> Because so much information is so readily available, there are extensive rules in place that lay out specific circumstances under which government investigators may access certain pools of information.

An investigation of a specific crime that has already been committed is far different than the government searching through data on a “fishing expedition” looking for suspicious activity. Ongoing surveillance is rightfully subjected to a wide variety of controls. But it is important that those controls not be too stringent. A strong case can be made, for example, that an overzealous concern for privacy hindered federal agents from uncovering information that might have helped unravel the September 11th attacks before they were carried out.<sup>10</sup> There is room for reasonable disagreement over how strict the controls should be, according to the circumstance. The government cannot, for example, conduct a drug raid on your house without reason to believe that drugs are in your house, but federal agents are allowed to use computers to sift through random collections of banking data looking for patterns that suggest money laundering, even if they do not know how or where the laundering is taking place. No matter where one feels the line should be drawn, the essential fact remains: There is a clear difference between investigating a crime and conducting surveillance. Lumping these two distinct activities together, as many in the civil liberties and privacy communities do, brings unnecessary confusion to the debate about governmental use of technology and its effect on citizens’ reasonable expectations of privacy.

### **3. Government data requires more stringent privacy protection than privately held data.**

There is no doubt that increased exchange of personal data—the kind of information about personal habits and preferences that privacy advocates consider sacrosanct—has boosted economic growth. By targeting individual customers based on their known preferences or demographic information, companies can greatly reduce their marketing costs. That information, therefore, is widely traded: A subscription to a

golf magazine is likely to get you placed on the mailing list for numerous golf merchandise catalogs. Similarly, filling out a product registration card for a computer game may fill your mailbox or email inbox with advertisements for new products in the future. Most Americans, to the extent they worry about it at all, consider this a minor nuisance or “junk mail” problem rather than a serious privacy violation. Most reputable companies, moreover, will give consumers who do worry about it the chance to “opt out” of this data trading.

Certain types of data, however, are more sensitive and subject to stricter regulation. Health information is generally given a very high level

of privacy protection.<sup>11</sup> Financial information is also highly protected as a general rule.<sup>12</sup> One reason that these types of information are protected is that an individual has no choice but to divulge such data and to allow it to be shared under the appropriate circumstances. A patient must give sensitive information to a doctor in order to receive effective treatment. Every American has his or her payment history reported to the credit bureaus without recourse, since an “opt out” on credit information would essentially destroy the entire system.

These same reasons apply to information given to the government. Personal information collected by government agencies demands more stringent protection because citizens are required to divulge the information, because they may not opt out of any authorized uses of the information, and because the information can be used to take away their rights. This is a long-standing principle of government information collection, as reflected in the federal government’s Privacy Act<sup>13</sup> and countless fed-

---

***“Technology tools can just as easily be used to empower citizens to observe their government in action.”***

---

eral and state regulations and laws governing the collection and use of information, from Social Security numbers to driver's license data. The use of information technology to collect or manage this information more efficiently has no bearing on this important privacy principle.

#### **4. Government use of new technology must be as transparent as possible to allow for accountability.**

Government secrecy has long been a source of visceral fear: Without a clear picture of how the government is operating, conspiracy theories and paranoia result. This is true of any form of government operation—as the Bush administration has proved time and again—but is particularly true when it comes to collection and use of personal information. Horror stories of domestic spies run amok under J. Edgar Hoover are part of the cultural and political landscape. The existence of new technologies—from software that reads email to miniaturized listening devices—tends to exacerbate such fears.

Transparency and sunshine have always been the best cure for the fears caused by government secrecy. Because information technology is privacy-neutral, the key is to deploy technology in a way that enhances government transparency and minimizes secrecy and abuses. Just as technology can be used to “spy” on citizens, it can also be used to spy on government employees to ensure that they are following the rules. Computerized security systems using smart cards or other physical “keys” can create logs indicating exactly where, when, and by whom data was accessed. Electronic “audits” can quickly scan the work of employees looking for anomalies that might indicate fraud, bribery, or just plain prurient curiosity (as was the case with the IRS employees who browsed through celebrity tax returns). Knowing that technology tools are being used to monitor their activities, government employees are much less likely to commit privacy abuses; the

days of browsing through tax returns or driving records will be over.

Technology tools can just as easily be used to empower citizens to observe their government in action. The Internet has been the next step in a long line of technology innovations designed to make the workings of government more accessible to the average taxpayer, from cameras in city council meetings to the terabytes of documents and data posted online by the White House, the Library of Congress, and federal departments and agencies. More and more state and local governments are following suit. This kind of transparency is not necessarily the ultimate goal of digital government. (Increased efficiency and improved service delivery constitute the next wave of digital transformation in the public sector.) But there can be little doubt that the easy availability of information about their government has let citizens become better aware of government activities. This transformation can continue only if governments keep digitizing their IT operations to make the information accessible in a way that paper documents can never match.

Meeting the goal of maximum transparency requires a concerted effort to implement both rules and systems that encourage scrutiny of technologies where there are privacy implications. Privacy audits conducted by independent third parties, legislative oversight, comment periods during system development, and the appointment of a chief privacy officer to each relevant government agency are just some of the ways that transparency can be enhanced. The key is a commitment to openness and the leadership to see that commitment through.

## **Privacy Principles in Practice**

Frequently in policy debates, the principles advocated by one side or the other get lost in micro-debates over details of a particular proposal. The risk of losing sight of the forest for

the trees is particularly strong in privacy debates, because the privacy implications of each detail of a given proposal tend to be evaluated in isolation, without consideration for how the details fit together in the overall system.<sup>14</sup> Because of this tendency, debates over specific legislative language can be less illuminating than a more general look at a government technology system and the attendant privacy implications. We therefore offer a general analysis of six controversial government technology programs to examine how the privacy principles detailed in this report should apply.

### ***The Computer Assisted Passenger Prescreening System (CAPPS II)***

The airline industry has long used computers to identify passengers as potential terrorist threats and single them out for particularly thorough scrutiny. Existing systems, however, rely on profiling of passengers against a presumed set of terrorist behaviors—purchasing one-way tickets, paying with cash, failing to check luggage, and so on. These systems are inefficient (flagging as many as 15 percent of passengers as terrorist threats) and ultimately do not work. Only nine of the 19 September 11th hijackers were flagged, and all were allowed to board their planes.<sup>15</sup>

To fix these flaws, the Transportation Security Administration (TSA) proposed developing a second-generation technology, CAPPS II. The new system would have taken personal information about passengers and compared it to private databases—of the type used to compile mailing lists for marketers—and to government databases of suspected terrorists. Taken together, such information could present a picture of a passenger as a long-time resident of the United States with no criminal history, and therefore a very low risk for a terrorist threat.<sup>16</sup> The system would not have revealed any personal information to airline agents, but rather would have reported back a red, yellow, or green threat status. This proposed system, according to TSA,

would have flagged only one-third as many passengers, allowing security officials to conduct a more thorough screening of potential threats with the same resources.<sup>17</sup>

Without a doubt, such a system would have constituted a novel use of private information by the government. Allowing a government agency to browse through information collected by private entities with the possibility of denying travel privileges is rightly of concern to all Americans. On the other hand, September 11th proved that our existing level of airline security was profoundly inadequate. The balance of security and privacy in this instance is one that should be debated freely and completely. But in the case of CAPPS II, it was not; the government was less than forthcoming about what it was doing, and privacy advocates fanned fears of potential abuses.<sup>18</sup>

The aborted CAPPS II system is a perfect example not only of the difficulty in striking the proper balance between security and privacy, but also of the need to follow stringent principles when the government is collecting data. Passengers were not going to be allowed to opt out of these background checks if they wished to fly.<sup>19</sup> Because of this, the most stringent possible privacy protections should have been used, more stringent than the rules that governed the marketers when they assembled the information in private databases in the first place. Moreover, because access to transportation might have been denied based on the results of a computer search, it is critically important that the data in any such system be accurate, and easily correctible when a mistake is discovered.

According to the General Accounting Office, the Transportation Security Agency made very little progress in addressing these critical operation issues. Of the eight key issues that Congress ordered TSA to address—the need for an internal oversight board, accuracy of data, stress testing, abuse prevention, unauthorized access prevention, policies for operation and use, privacy concerns, and redress process—only the

---

first had been fully addressed.<sup>20</sup> In part because of the failures of the administration to address these issues, and in part due to pressure from privacy advocates, the administration made a decision to stop work on the system.

### ***Terrorist Information Awareness and Data Mining***

Perhaps the biggest government privacy controversy in recent memory surrounded the Terrorist Information Awareness (TIA) project. At least part of the controversy can be blamed on the fact that the project was originally named “Total Information Awareness,” a public relations mistake that was quickly rectified. But the true roots of the controversy were more substantive: TIA represented the first effort by the federal government to use computers to conduct mass surveillance on people.

In one sense, this substantive controversy was overblown. Far from being implemented, the TIA project was never more than an early-stage research project by a Defense Department

technology lab.<sup>21</sup> The system was never even close to being put into operation, it was merely being tested and developed. Moreover, many

technology experts believe that the current capabilities of the TIA program are so limited that it is not “scalable”—that is, it is unable to be expanded to analyze large amounts of data—and therefore the idea that it will achieve “total information awareness” is a distant dream at best. Nevertheless, the issues raised by the TIA project—and data mining in general—need to be confronted.

The basic concept of data mining is to use computers to examine large amounts of data in order to identify patterns that might not be obvious to human analysts. The technology has long been in use by corporations mining their own data in an effort to discern more efficient business strategies. For example, they may discover that customers who buy a particular product are more susceptible to a particular marketing pitch than others. In the government realm, data mining has been used in efforts to spot money laundering.<sup>22</sup>

As conceived in the TIA project, the data mining for anti-terrorist efforts would have been entirely in keeping with the first principle described in this paper: An increase in efficiency is not, by itself, an invasion of privacy. The TIA project merely sought to analyze data (public and private) already properly acquired by the government, which is already subject to existing rules on access and usage. The advance would have come in combining data that is ordinarily separated by bureaucratic stovepipes. There would have been no increase in government authority to collect or examine data; the increase would only have been in the ability to “see” all the data at one time.

Given the existing set of rules covering information access and usage—and especially given the clear need to more effectively “connect dots” that may point to terrorist activity—data mining by government is not only a fair privacy trade off but a necessary one. Though the TIA project itself may never have been successful (or may never have been cost-effective), our future homeland security depends on breaking down stovepipes and creating a network—constrained by rules to prevent abuse—that allows data to flow more freely and be analyzed by trained agents using technology tools. A network of government information could greatly increase the chances of preventing terrorist attacks. Privacy can be assured in such a system if proper rules are established and Congress keeps a watchful

---

***“Given the existing set of rules covering information access and usage, data mining by government is not only a fair privacy trade off but a necessary one.”***

---

eye—as it has over CAPPs II and other government technology initiatives. With those proper constraints and oversight, data mining can be an important tool for making Americans safer.<sup>23</sup>

### ***Integrated Databases for State Motor Vehicle Departments***

The state-issued driver's license or identification card (DL/ID) is the most widely used and accepted form of identification in America today. The DL/ID can be used for almost every conceivable government transaction, including securing other forms of identification such as a passport. It is also used in virtually every commercial or private transaction requiring proof of identification or age, from opening a bank account, to renting an apartment, to buying a beer.

Unfortunately, DL/ID's are also frequently falsified and forged. (A false DL/ID is a card obtained from a state DMV with false information, but is otherwise valid. A forged DL/ID is a realistic-looking card that is created completely outside of the DMV.) With the easy availability of high-resolution color printers and Internet access, it is possible to create an official-looking DL/ID from, say, the state of Michigan and pass it off to bartenders and bank tellers in Texas or Maine—a Michigan resident might recognize the forgery, but residents of other states have no way of telling. This forgery problem could be mitigated—though not solved—if every state agreed to include a standard feature on their cards, such as a hologram of an eagle.<sup>24</sup>

The false DL/ID is a much tougher problem to solve. Generally, a false DL/ID is obtained with false “breeder documents” such as a forged birth certificate, or, more rarely, through bribery of a DMV employee. Once a false DL/ID is obtained, the door is opened to any number of criminal activities, from identity theft to terrorism. (Several of the September 11th hijackers had false DL/IDs obtained by bribing someone for forged breeder documents.) More typically, acquiring a false DL/ID is done for the purpose of underage

drinking, or to avoid “points” accrued for traffic violations on a driver's license in another state.

One way to reduce the risks of false DL/IDs would be to allow each state to query the DL/ID databases of other states before issuing a DL/ID. This would discourage people from attempting to apply for multiple cards in different states, a process that is altogether too easy under the current system. This multi-state check has been in place for over a decade for commercial driver's licenses. The Commercial Driver's License Information System (CDLIS) uses a “pointer system” to allow state DMVs to query other DMVs regarding the status of license applicants.<sup>25</sup> The American Association of Motor Vehicle Administrators (AAMVA), the operator of the CDLIS system, has proposed to expand the pointer system to all DL/IDs under a program called the Driver Record Information Verification System (DRIVERs).

But this effort has been met with a barrage of criticism from privacy advocates. The most common argument is that linking the state databases together will create a “national ID card” that somehow violates privacy by turning the United States into a “show us your papers” nation.<sup>26</sup> This criticism is wrongheaded for a number of reasons. First, it conflates the state DL/ID, which is voluntary (no one is required to obtain a driver's license), with the vague concept of “national ID card” that is generally taken to mean an identification document issued by the federal government that is mandatory for all citizens to carry at all times.<sup>27</sup> Second, it ignores the reality that the DL/ID is already accepted as proof of identification across the nation, despite the widespread knowledge that false or forged cards are so commonplace as to be almost a rite of passage. Merely securing the system to eliminate fraud will not move the nation any closer to a “national ID card” any more than we now have a national commercial driver's license.

The main reason that this criticism is misguided, however, is that linking the DMV databases together does not alter the privacy tradeoff

for citizens one iota. Linking the databases would not require individuals to turn over more personal information, and it would not grant any additional authority to any government agencies, which are already free to verify any information provided to them with a phone call. (When applying for a DL/ID, applicants must either declare which state they currently hold a card, or affirm that they do not currently hold a card, and the issuing DMV can verify that information.)

---

**“Despite the fact that the red light cameras do not perform any function that could not be performed by a uniformed police officer, many privacy advocates resort to extreme hyperbole to describe their impact.”**

---

The fact that a database pointer system would make this verification process much more efficient and less costly does not, in and of itself, constitute a privacy violation. Of course, the rules of the system need to be established to ensure that the database system is not used to violate privacy. AAMVA has already established a set of privacy principles that will govern the development of any new technologies deployed to make the DL/ID system more secure.<sup>28</sup> A system of rules protecting privacy has already been put into place in the Social Security Online Verification system (SSOLV), which DMVs use to verify that an applicant is providing an accurate social security number. The system checks the databases of the Social Security Administration, but does not reveal any data to the state DMV; rather, it merely returns a “red light/green light” response.<sup>29</sup> The SSOLV system proves that cross-jurisdictional database checks can be implemented in a way that protects privacy while also improving the process. Proper security would also need to be in place to keep hackers from attacking the data.

## **Photo Traffic Enforcement**

Automated photo traffic enforcement systems—such as red light cameras and photographic radar guns—are tremendously unpopular in the United States, though they have been used in Europe for years. The devices are installed at intersections (or possibly mounted in vehicles so they can be deployed to different spots on different days) to take photographs of vehicles that run through red lights or exceed the speed limit, so that a citation can be sent to the registered owner of the vehicle through the mail. Because the devices can be deployed without a police officer present, and because they can immediately restart their “patrols” since no time is wasted pulling over a driver and filling out a paper citation, photo enforcement is becoming increasingly popular with local governments.<sup>30</sup>

But a number of objections have been raised to photo enforcement devices, and in many cases the objections have kept the devices from being deployed. Detractors contend that the equipment’s use by private contractors creates a conflict of interest, that the devices actually harm traffic safety by encouraging drivers to slam on their brakes, and that they create a presumption of guilt against which cited drivers must prove their innocence (especially if the citation is sent to the vehicle’s owner, who may not have been driving the vehicle at the time of the violation). Some detractors even believe that yellow-light cycles are manipulated in order to trick more people into running red lights; or, at the very least, that contractors deploy the cameras at intersections most likely to generate revenue.<sup>31</sup> These are all legitimate implementation issues that do not relate to privacy. The objections of privacy advocates have less merit.

Despite the fact that the red light cameras do not perform any function that could not be performed by a uniformed police officer, many privacy advocates resort to extreme hyperbole to describe their impact. Former Rep. Dick

Arme y (R-Texas) referred to the devices as “Orwellian cash machines.”<sup>32</sup> Former Rep. Bob Barr (R-Ga.) echoed the sentiment: “At traffic intersections in cities large and small, from Washington, D.C. to Marietta, Georgia in my own district, Americans are being watched, their movements recorded, their persons and surroundings photographed, and their actions documented by their government; even as they are often unaware they are being monitored by their government and unable to do anything about it even if they are . . . The question is whether we will choose the future of American society to be an Orwellian one.”<sup>33</sup> Columnist Eric Peters declared: “The same equipment that can be used to catch red light runners can also easily be used to keep track of your movements, identify and catalog who you happen to be traveling with, and so on.... It’s not much farther to a society in which ‘Your papers, please!’ becomes as accepted as it was in Soviet Russia or Nazi Germany.”<sup>34</sup>

The fallacy common to all of these arguments is the idea that using cameras for traffic enforcement is a *per se* violation of privacy. Nobody can doubt the authority of police officers to observe drivers as they move down the road or through intersections. Using cameras to do the same job does not alter the authority possessed by the government, nor does it alter the privacy rights of citizens. The cameras are merely a more efficient way of exercising existing authority.

Moreover, privacy advocates often fail to recognize the difference between investigation and surveillance. The cameras are not used to “track” the movements or behaviors of drivers; no data is recorded until a violation is detected. In that sense, the cameras do not even make very good investigative tools; unlike, say, the cameras in convenience stores, red light cameras cannot be used to reconstruct the actions of anyone who passes through an intersection unless that person happened to run a red light. Any discussion of the cameras being “the first installation of the Big Brother infrastructure” merely points out the

importance of having appropriate rules governing the use of the technology, but does not argue against the technology itself.<sup>35</sup>

An example of photo traffic enforcement from Europe is instructive of how such technology can be deployed while being sensitive to privacy. In London, traffic cameras with license plate recognition software are used to enforce “congestion charging,” a system that requires motorists to pay for the right to bring a vehicle into central London during the busy part of the day. The object is not to raise revenue, but to encourage the use of public transportation by raising the cost of driving a car in the central city. The system was deployed over a year ago, despite objections by privacy advocates, and has worked very well. A key to the system is the data retention policy that has been put in place; the database automatically deletes any images of motorists who have already paid the congestion fee, and it saves images only for those who decide at the last minute to drive downtown or who ignored the law. A reminder is sent to anyone in the latter category, and the record is erased when the fee is paid.<sup>36</sup> The London system is a perfect example of how technology can enhance efficiency—it completely eliminates the need for lines at dozens of tollbooths—yet be properly designed to balance privacy against that efficiency.

### **DNA Databases**

The leading edge of law enforcement technology in the 21st century is the use of DNA identification to solve crimes. When analyzed properly, DNA can match, with almost perfect accuracy, an individual to evidence left at a crime scene, such as blood, semen, hair, saliva, or skin. The technology has not only been useful in cracking otherwise unsolvable cases,<sup>37</sup> but it has also been an invaluable tool in freeing individuals who were wrongly convicted of crimes.<sup>38</sup> Far more accurate and flexible than mere fingerprinting, DNA identification is one of the most powerful

tools currently available to our justice system.

In order to harness the full power of DNA identification, however, a database similar to the fingerprint database must be established. DNA can be used in any instance for “one to one” matching; that is, matching evidence of a particular crime with a particular suspect to see if the suspect was at the crime scene. But the true power of DNA identification occurs when there is no suspect, only DNA evidence. By running the DNA evidence against a database of DNA samples, a criminal may be found.

The easiest way to do this, of course, would be to require every citizen to turn over a DNA sample. But it is widely recognized that such a step goes too far in the tradeoff between privacy and justice. (It is why we have never had mandatory fingerprinting of all citizens.) The concern over DNA samples is further justified because the potential for abuse is higher than with fingerprints, since a DNA sample can be used not only for identification, but to learn facts about an individual’s genetic makeup and medical conditions. Instead, only a small subset of individuals must turn over DNA samples for inclusion in a database, just as only a small subset of individuals currently turns over their fingerprints for inclusion in a database. The dilemma is deciding which subsets must turn over samples.

For simple fingerprints, the rule is well established: Anyone arrested and booked on suspicion of any crime must be fingerprinted. It does not matter what the crime is, or whether the suspect is found guilty (or even indicted). Collection and storage of fingerprints is routine in any arrest. This is a system that could lend itself to possible abuses (such as making an arrest on false pretenses simply to acquire fingerprints), but by and large the rules have worked well over the past several decades.

DNA samples, on the other hand, are collected from a much smaller subset of individuals. Rules vary from state to state, but a typical rule would be that DNA samples are

collected only from those individuals who are convicted of a violent felony (perhaps further restricted to felonies involving a sex offense). These rules are in place, in some cases, for purely operational reasons; collecting and processing DNA samples is expensive, and collecting a sample from a convicted sex offender is more likely to turn up a “hit” on another cold case than collecting a sample from somebody arrested for, say, marijuana possession. The cost-benefit analysis may justify limited collection, therefore, but such limitations are not justified on privacy grounds. If proper rules and procedures are in place to ensure that a DNA sample is used the same way a fingerprint is used—for identification by law enforcement only, and not for the extraction of additional genetic information—then there is no privacy basis for being more restrictive on DNA collection than on fingerprint collection.

Just as privacy concerns have hampered the collection of DNA samples, they have also hampered the creation of a nationwide DNA database to match the functionality of the FBI’s fingerprint database. The Combined DNA Index System (CODIS) began as a pilot program in 1990 and has now expanded to include 48 states and the District of Columbia (Mississippi and Rhode Island do not participate).<sup>39</sup> There are no national standards, however, governing the collection of samples or the submission of samples to CODIS; Arizona and Colorado, for example, have similar size populations, but Arizona has submitted four times as many forensic samples to CODIS.<sup>40</sup> The House of Representatives passed a bill to standardize both the rules for putting DNA samples into the database and the process for convicted inmates to have DNA tested to prove their innocence, but the bill is currently awaiting action in the Senate.<sup>41</sup> This is yet another instance where privacy concerns are limiting government efficiency in an inappropriate way.<sup>42</sup>

---

## **Public Records**

It goes without saying that the proceedings of government, from town hall meetings to Supreme Court arguments, ought to be open to the public. It becomes more questionable when government records involve information about individual citizens. Most information held by government pertaining to individual citizens is protected by a variety of privacy laws. There are, however, large classes of individual information that are held as public records for the protection of all citizens. Public arrests and trials guard against a police state where citizens simply disappear in the middle of the night. Public property records guard against unfair or discriminatory taxation of property. Vital records (birth, death, and marriage) help protect against fraud.

Access to public records used to be cumbersome at best. Information often ran in newspapers, but was not organized in any way to search for individuals. Records were also available in the form of photocopies that could be obtained by visiting local government agencies. Public records, in other words, were not all that public. The Internet has changed that. Now many jurisdictions allow free searches of home values, and online searches of criminal history databases are inexpensive and instantaneous. Moreover, as public records, they contain bare facts but no context; for example, the “sex offender” databases made available online by many jurisdictions rarely differentiate between rapists, child molesters, and those convicted under antiquated laws for consensual relations with a member of the same sex. This changes the outlook on “public” information, particularly for the many thousands of Americans who may have hoped that their marijuana bust in college or the unfortunate entanglement in a prostitution sting were firmly in their past.<sup>43</sup> As a result, privacy groups and others have scrutinized the amount of in-

formation that is available, and in what form, in public records.

The Internet has changed the way people feel about public records, but if the electorate collectively wishes to do something about it, the appropriate action is to change the nature of the public records, not limit the technology that can be used by government to organize and maintain those records. That is, public records should not be maintained on paper in file drawers for the sole purpose of protecting pri-

privacy; data can be digitized without being placed on the Internet. Legislating changes to the accessibility of public records may or may not be desirable.<sup>44</sup> Denying governments the right to use effective technology tools is always undesirable.

## **Conclusion**

Modern information technology has the power to transform governments at all levels to make them far more effective, efficient, and responsive to citizen needs. These powerful tools also harbor the potential to threaten the privacy and freedom of every American citizen. But rather than fear technology because of potential abuses, governments should devote their efforts to deploying these tools in ways that protect our privacy as citizens while allowing us to reap the benefits as taxpayers.

---

***“The Internet has changed the way people feel about public records, but if the electorate collectively wishes to do something about it, the appropriate action is to change the nature of the public records, not limit the technology that can be used by government to organize and maintain those records.”***

---

## Endnotes

<sup>1</sup> “CAPPS II Data-Mining System Will Invade Privacy and Create Government Blacklist of Americans, ACLU Warns,” *ACLU*, Press Release, February 27, 2003, <http://www.aclu.org/Privacy/Privacy.cfm?ID=11956&c=130>.

<sup>2</sup> Atkinson, Robert D., and Jacob Ulevich, “Digital Government: The Next Step to Reengineering the Federal Government,” *Progressive Policy Institute*, March 2000, <http://www.ppionline.org>; Leigh, Andrew and Robert D. Atkinson, “Breaking Down Bureaucratic Barriers: The Next Phase of Digital Government,” *Progressive Policy Institute*, November 2001, <http://www.ppionline.org>.

<sup>3</sup> See, for example, <http://faculty.knox.edu/fmcanadre/evoloresearch.html>.

<sup>4</sup> For a detailed history of the credit reporting industry, see <http://www.phil.frb.org/pccldiscussion/historycr.pdf>.

<sup>5</sup> National Crime Information Center, <http://www.fbi.gov/hq/cjisid/ncic.htm>.

<sup>6</sup> Some scholars, including ethics professor Richard O. Mason, believe that privacy arises from the Western tradition of humanism, though the concepts need to be stretched to be linked, <http://cyberethics.cbi.msstate.edu/mason2/>.

<sup>7</sup> “Google Date Test ‘Nets U.S. Fugitive,” *BBC News*, January 30, 2004, <http://news.bbc.co.uk/1/hi/world/americas/3445523.stm>.

<sup>8</sup> “Your Papers, Please: From the State Driver’s License to a National Identification System,” *Electronic Privacy Information Center*, February 2002, <http://www.epic.org/reports/yourpapersplease.pdf>. Also, see the coalition letter to President Bush opposing the creation of a “national ID card.” <http://www.aclu.org/Privacy/Privacy.cfm?ID=13602&c=130>. In addition, see [http://www.epic.org/privacy/id\\_cards/ncidletter6.27.02.html](http://www.epic.org/privacy/id_cards/ncidletter6.27.02.html)

<sup>9</sup> This power can become increasingly dubious as the crime decreases in importance. The classic example is Whitewater Special Prosecutor Kenneth Starr subpoenaing the book purchase records of a White House intern.

<sup>10</sup> Stuart Baker, former general counsel to the National Security Agency, has made this argument with respect to the “wall” between intelligence activity and law enforcement activity: <http://slate.msn.com/id/2093344>.

<sup>11</sup> *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, P.L. 104-191, <http://aspe.hhs.gov/admsimp/pl104191.htm>. Some might argue that health information is given too much protection, to the point that it interferes with the free flow of data between doctors, specialists, pharmacists, and other providers.

<sup>12</sup> There are other subsets of “personal information” that get varying degrees of legal protection, from the virtually iron-clad protection of attorney-client communications, to strict rules protecting credit reporting data in the Fair Credit Reporting Act (Public Law 91-508), to the rules prohibiting disclosure of titles rented from a video store in the Video Privacy Protection Act of 1988 (Public Law 100-681).

<sup>13</sup> *The Privacy Act of 1974*, 5 U.S.C. § 552a, <http://www.usdoj.gov/foia/privstat.htm>.

<sup>14</sup> For example, privacy advocates might decry “spyware” placed on the computers of government workers without considering whether the software is designed to prevent those employees from abusing the privacy of citizens whose data they possess.

<sup>15</sup> The flagged hijackers had their luggage checked for explosives and were allowed to board once the luggage was determined to be clean. Mittelstadt, Michelle, “Security Officials Searched Luggage, Not Hijackers, Panel Hears,” *Kansas.com/The Wichita Eagle*, January 27, 2004, <http://www.kansas.com/mld/kansas/news/politics/7810625.htm>.

<sup>16</sup> “CAPPS II At a Glance,” *Transportation Security Administration, U.S. Department of Homeland Security*, February 20, 2004, [http://www.tsa.gov/public/interapp/tsa\\_policy/tsa\\_policy\\_0035.xml](http://www.tsa.gov/public/interapp/tsa_policy/tsa_policy_0035.xml).

<sup>17</sup> Goo, Sara Kehaulani, “U.S. to Push Airlines for Passenger Records,” *The Washington Post*, January 12, 2004, <http://www.washingtonpost.com/wp-dyn/articles/A8504-2004Jan11.html>

<sup>18</sup> The TSA collected public comments on the privacy issues surrounding CAPPS II; the compilation can be found at [http://www.dhs.gov/interweb/assetlibrary/CAPPSII\\_Letters\\_110703.pdf](http://www.dhs.gov/interweb/assetlibrary/CAPPSII_Letters_110703.pdf).

<sup>19</sup> Of course, it is possible to opt out of the background check by not flying, but airlines have become an indispensable part of the transportation system and are integral to the freedom of movement every citizen enjoys. As such, airline travel can fairly be considered an essential service, much like telephone service is essential to everyday life.

<sup>20</sup> “Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges,” *U.S. General Accounting Office*, February 2004, <http://www.gao.gov/new.items/d04385.pdf>.

<sup>21</sup> “Report to Congress Regarding the Terrorism Information Awareness Program,” May 20, 2003, <http://www.eff.org/Privacy/TIA/TIA-report.pdf>.

<sup>22</sup> “Treasury’s Mining for Crooks,” *Government Computer News*, August 18, 2004, [http://www.gcn.com/vol19\\_no10a/enterprise/1838-1.html](http://www.gcn.com/vol19_no10a/enterprise/1838-1.html).

<sup>23</sup> Law professor Jeffrey Rosen, a well-known privacy advocate, believes that data mining can be an appropriate tool: <http://reform.house.gov/UploadedFiles/Rosen%20testimony.pdf>.

<sup>24</sup> For a far more detailed look at the steps needed to make the state DL/ID system more secure, see Ham, Shane, and Robert D. Atkinson, “Modernizing the State Identification System: An Action Agenda,” *Progressive Policy Institute*, February 2002, <http://www.ppionline.org>.

<sup>25</sup> “Commercial Driver’s License Information System,” *American Association of Motor Vehicle Administrators*, 2001, [http://www.aamva.org/drivers/drv\\_AutomatedSystemsCDLIS.asp](http://www.aamva.org/drivers/drv_AutomatedSystemsCDLIS.asp).

<sup>26</sup> “Coalition Letter to President Bush Urging Him to Reject National ID Card,” *American Civil Liberties Union*, February 11,

---

2002, <http://www.aclu.org/Privacy/Privacy.cfm?ID=13602&c=130>.

<sup>27</sup> This is sometimes derided as “permission to live.” <http://bureaucrash.com/campaigns/iamnotanumber/>.

<sup>28</sup> “Status Report to AAMVA Membership,” *American Association of Motor Vehicle Administrators*, July 2003, <http://www.aamva.org/Documents/idsAttach4StatReportJuly03.pdf>.

<sup>29</sup> Lockhart, III, James B., “Testimony Before the Senate Finance Committee: Hearing on the Homeland Security Threat from Document Fraud,” 108th Congress, September 9, 2003, [http://www.ssa.gov/legislation/testimony\\_090903a.htm](http://www.ssa.gov/legislation/testimony_090903a.htm).

<sup>30</sup> In fact, the process is so efficient that private contractors find it profitable to deploy the systems at no cost to government, receiving payment through a percentage of each paid citation.

<sup>31</sup> For the definitive indictment of photo traffic devices, see the April 2002 five-part series by *Weekly Standard* senior writer Matt Labash, <http://www.weeklystandard.com/Content/Public/Articles/000/000/001/078ftoqz.asp?pg=1>

<sup>32</sup> “Orwell’s Cash Machine Out of Service in San Diego,” *Highwayrobbery.net*, May 25, 2001, <http://www.highwayrobbery.net/TickRedCamArmeyorwellatm.asp>

<sup>33</sup> Barr, Rep. Bob, “Testimony Before the U.S. House of Representatives Committee on Transportation and Infrastructure, Subcommittee on Highways and Transit,” 107th Congress, July 31, 2001, <http://www.house.gov/transportation/highway/07-31-01/barr.html>.

<sup>34</sup> Peters, Eric, “Red-Light Cameras Violate Our Privacy and Can Be Used to Entrap the [sic],” *Idea House, National Center for Policy Analysis*, 2001, <http://www.ncpa.org/bothsideside/krt/krt061401a.html>.

<sup>35</sup> Jim Harper, editor of *Privacilla.org*, made this same point in testimony to a House subcommittee: [http://www.privacilla.org/releases/red-light\\_camera\\_testimony.html](http://www.privacilla.org/releases/red-light_camera_testimony.html).

<sup>36</sup> For a more detailed explanation of how the system works, see <http://www.roadtraffic-technology.com/projects/congestion>.

<sup>37</sup> “DNA Database Helps Clear Two ‘Cold’ Homicide Cases,” *Lawrence Journal-World*, February 2, 2004, <http://www.ljworld.com/section/stateregional/story/160005>.

<sup>38</sup> “DNA News,” *The Innocence Project*, August 18, 2004, <http://www.innocenceproject.org/dnanews/index.php>.

<sup>39</sup> “Participating States,” *Combined DNA Index System, Federal Bureau of Investigation*, <http://www.fbi.gov/hq/lab/codis/partstates.htm>.

<sup>40</sup> “NDIS Statistics,” *Combined DNA Index System, Federal Bureau of Investigation*, <http://www.fbi.gov/hq/lab/codis/clickmap.htm>.

<sup>41</sup> The Advancing Justice Through DNA Technology Act of 2003 (H.R. 3214 and S. 1700 in the 108th Congress) are both languishing in the Senate Judiciary Committee as of this writing.

<sup>42</sup> For a summary of the privacy arguments against expanding CODIS, see <http://archive.aclu.org/congress/1032300a.html>.

<sup>43</sup> In many cases, a record of a minor criminal violation for a non-habitual offender can be expunged, but there is usually a delay of many years before expungement.

<sup>44</sup> For instance, universal digitization of property records could greatly reduce the cost of title insurance, saving homebuyers billions of dollars every year. For more see Ham, Shane, and Robert D. Atkinson, “Modernizing Home Buying: How IT Can Empower Individuals, Slash Costs, and Transform the Real Estate Industry,” *Progressive Policy Institute*, March 2003, <http://www.ppionline.org>.





*Find this and other policy reports at*  
**www.PPIONLINE.org**, the official website of  
the Progressive Policy Institute.

---

## **Now on PPIonline.org:**

- Meeting the Offshoring Challenge**  
Robert D. Atkinson
- Understanding the Offshoring Challenge**  
Robert D. Atkinson

## **Also from the PPI Technology and New Economy Project:**

- Digital Government: The Next Step to**  
Reengineering the Federal Government  
Robert D. Atkinson
  - Modernizing the State Identification System:**  
An Action Agenda  
Robert D. Atkinson
- 

*If you would prefer to receive future reports  
via email, please contact the PPI  
Publications Department at*  
**publications@dlcppi.org**