Center for American Progress

The ID Divide

Addressing the Challenges of Identification and Authentication in American Society

Peter P. Swire and Cassandra Q. Butts

June 2008

www.americanprogress.org
Progressive Ideas for a Strong, Just, and Free America

The Progressive Identity Project

The Progressive Identity project arose from the recognition that the next administration will face identification and authentication issues in a wide range of contexts. Americans are increasingly being asked to identity themselves, both in person and online. The goal is to try to set forth principles and insights that will provide a coherent approach for diverse issue areas such as:

- ***National and homeland security***. The REAL ID Act and numerous other identification programs have been proposed since the attacks of September 11, 2001

- ***Immigration***. There have been prominent debates about identity requirements at the time a person starts a job and about government-issued IDs for non-citizens

- ***Voting***. The last few years have seen unprecedented state laws requiring ID to vote, and subsequent litigation about those laws' constitutionality

- ***Electronic health records***. It remains unclear how to accurately and securely link a patient's health records, held by different providers, as the system shifts to electronic medical records

- ***Online authentication***. Many new approaches are underway for authenticating users online, both for e-government and e-commerce

- ***Computer security***. Many computer security experts have argued that identification systems proposed to promote security can instead create new security risks

- ***Privacy and civil liberties***. New identification systems, especially if they are badly designed, can pose serious problems for individual privacy and civil liberties

To study these issues of identification and authentication, we convened a group of experts* from all of the issue areas listed above for an intensive one-day meeting in November, 2007. The emphasis was on learning across issue areas because most previous debates on identification and authentication have occurred in isolation with limited cross-fertilization of ideas among experts. The group convened for a second meeting in March, 2008.

When the next administration takes office in January, 2009, it will need to make new policy going forward on numerous identification and authentication issues. The new administration will also have the first opportunity since the terrorist attacks of September 11, 2001 to examine decisions made since then in the light of nearly a decade of experience. We believe this report will help the new administration tackle this critical issue early and swiftly, preparing our country for the challenges to civil liberties and national security posed by the complex issues of identification and authentication.

For the online resource page for the Progressive Identity project, visit http://www.americanprogress.org/issues/2008/06/id_resources.html .

* ***The list of participants who wished to be listed is included in the appendix. The Center for American Progress warmly thanks all of the participants in this collaborative project.***

THE ID DIVIDE

Addressing the Challenges of Identification and Authentication in American Society

Peter P. Swire and Cassandra Q. Butts

Center for American Progress

June 2008

Introduction and Summary

How individuals identify themselves in our country grows more complex by the year. Just last month, 12 nuns were turned away from voting booths during the Indiana presidential primary because they lacked state identification (none of them drives), a stark reminder that the recent Supreme Court ruling that upheld Indiana's voter ID law poses lasting consequences to our democracy. And two years ago last month the personal data of 26.5 million veterans were lost from a government laptop, the latest in a series of data breaches that threaten the integrity of everyone's identification.

Those 12 nuns are among 20 million other voting age citizens without driver's licenses, and they join those 26.5 million veterans and many millions of other Americans who suddenly find themselves on the wrong side of what we call the ID Divide—Americans who lack official identification, suffer from identity theft, are improperly placed on watch lists, or otherwise face burdens when asked for identification. The problems of these uncredentialed people are largely invisible to credentialed Americans, many of whom have a wallet full of proofs of identity. Yet those on the wrong side of the ID Divide are finding themselves squeezed out of many parts of daily life, including finding a job, opening a bank account, flying on an airplane, and even exercising the right to vote.

For many reasons, the number of ID checks in American life has climbed sharply in recent years, especially in the wake of the 9/11 terrorist attacks on our country in 2001. In fact, the growing ID Divide is similar in many ways to the "Digital Divide" that exists for those who lack access to computers and the Internet, which in turn leaves them without access to numerous opportunities for education, commerce, and participation in civic and community affairs. The ID Divide leaves those without proper means of identification or with compromised ID unable to participate in the most basic functions of everyday life in our economy and democracy.

What's worse, Americans and their representatives in government at the federal, state, and local levels are divided about what to do about these problems. Some want stricter identification systems, most prominently to fight terrorism and to limit immigration. Their voices are joined by those who see massive profits to be had if the United States embraces ever more intrusive forms of personal identification—beyond fingerprints to iris scans, embedded ID chips, DNA profiles, and other forms of ID that, combined with personal and public financial records, would in fact throw more and more Americans onto the wrong side of the ID Divide. Others have a starkly different view. They are skeptical in general of new programs that require proof of ID, for cost, computer security, privacy, and civil liberties reasons.

These divisions are most visible in recent debates about whether the REAL ID Act, which would set strict federal standards for states to follow in issuing driver's licenses, would create a national ID system and should be implemented. The Department of Homeland Security has proposed regulations to implement REAL ID, but the next administration will face crucial choices about whether, or how, to continue with that approach.

Amid this debate, we recognize that there are circumstances where strong identification is required in the service of certain goals, such as national and homeland security. But in light of the many problems that can arise from use of identification, we support a process of careful vetting, or "due diligence" (to borrow a phrase from the financial world) for any new ID proposals. There should be scrutiny on cost and technical feasibility. There should be a detailed examination of whether an authentication procedure is reasonable given the goals rather than simply feasible because a new way to identify an individual is now possible.

In particular, we believe such due diligence would illustrate that many of the claims of ID vendors and other identity system proponents do not stand up well to such scrutiny. Fingerprint-based systems, for example, have much greater long-term flaws than most proponents and observers understand—and this form of ID has been around for decades. Due diligence

Progressive Principles for Identification Systems

The Progressive Identity project is "progressive" in that it seeks to frame a pragmatic set of solutions driven by facts, not ideology, in a way that benefits the community as a whole, while ensuring that all people are treated fairly and equally. A progressive approach to identification systems looks at the effects on society as a whole, and does not focus simply on the convenience of those administering the system.

As a policy matter, there are two distinct steps in assessing possible identification systems: Whether to create the system at all, and if so, how to do it. In practice, these two steps often merge, because the overall desirability of a system depends in large part on how it is implemented. The principles here thus can be usefully applied to both steps of the policy process. In response to the ID Divide, the project has thus identified six principles for identification systems.

Achieve real security or other goals
New identification systems proposed in the name of security should be subject to a due diligence review to ensure that they actually promote security and do so cost-effectively compared to other available options. Similarly, identification systems proposed for other purposes, such as immigration policy, should only be deployed after they are shown to be effectively related to achieving the specified policy goals. This principle comes first for a simple reason—the financial and other costs of a new system are justified only if they actually achieve security or other goals. If they do not, then the analysis should end at this step.

Accuracy
A system will only work in the long run if it has a high level of accuracy. Any system, such as a watch list, has "false positives" (people treated as terrorist suspects mistakenly) and "false negatives" (people who are dangerous who evade detection by the system). A proposed system should be carefully vetted to ensure that the accuracy produced by the system will result in a manageable number of false positives and negatives.

Inclusion
As ID checks spread, it becomes increasingly important to ensure that people have a workable way to reduce the effects of the ID Divide. In many instances, there may be opportunities to rely on authentication approaches other than full identification. Where identification is used, however, then a goal of the policy process should be to foster inclusion of eligible persons.

must also include careful consideration of other important values, including: unequal effects on the poor and other disadvantaged groups; avoidance of excessive and uncompensated burdens on individuals (such as those wrongly put on watch lists); and burdens on important rights including privacy and the right to vote.

Our report first explores the background of the issue, including the sharp rise in recent years in how often Americans are asked for proof of identity. We then examine the facts of the ID Divide in detail, identifying at least four important types of problems:

- A large population affected by identity theft and data breaches
- The growing effects of watch lists
- Specific groups that disproportionately lack IDs today
- The effects of new and stricter ID and matching requirements

These problems raise clear reasons for caution about implementing identification systems, which often have large, negative effects on those on the wrong side of the ID Divide. When systems need to be implemented, these problems show the great importance of designing systems with policies to address them. We argue that a strong set of progressive principles for identification systems (see sidebar below) must first determine whether to create the system at all; and if so, how to do it. Those decisions should be based on:

Fairness and equality

New authentication and identification systems should be designed with consideration of their effects on the less wealthy and others who would suffer disproportionate burdens from any given design. Equality principles are especially important with respect to fundamental rights, such as the right to vote, and for any system where use of the ID is vital to daily tasks, such as opening a bank account or proving eligibility for a job. Where necessary, in order to enable people to live fully in society, fees should be waived based on financial hardship. Procedures for reasonable exceptions should also be developed, in recognition that any one method of identification will not work for the entire eligible population.

Effective redress mechanisms

Stricter and more numerous identification systems mean that burdens increase greatly on individuals who are mistakenly put on watch lists or otherwise disadvantaged by the system. An integral part of system design must be to have effective redress mechanisms. Otherwise, individuals will be turned into second-class citizens, deprived of the ability to conduct daily activities of life in a normal way. An effective security system must have not just on-ramps, but off-ramps as well. A properly designed system will allow government to distinguish between those who actually pose a threat and those who do not, and to proactively remove names from the watch list without a formal petition. If the security system remains the one-way street it is now, then it will inevitably collapse from its own weight.

Equitable financing for systems

A major criticism of the REAL ID Act has been its unfunded mandates. Congress has only provided the states with a small fraction of the expenses of implementing the federal requirements, now estimated at $4 billion over 10 years, but perhaps more. Along with such unfunded expenses to states and localities, REAL ID and other new identification systems impose off-budget costs on individuals who must spend time and money to meet the system's requirements. These include: tracking down birth certificates and other documentation; the time needed to try to resolve problems; and the costs to eligible individuals who get put on watch lists or otherwise cannot meet the system requirements. New identification systems, built for the common good, should thus be funded in a transparent and equitable way.

- Real security or other goals
- Accuracy
- Inclusion
- Fairness and equality
- Effective redress mechanisms
- Equitable financing for systems

How can these principles be honored in practice? That's where the "due diligence" process comes into play when considering and implementing identification systems. Due diligence in the financial world of mergers and acquisitions and other important corporate transactions is conducted before a company makes a major investment. Proponents of, say, a merger (or in our case, a new identification program) can err on the side of optimism, concluding too readily that the merger (or new ID program) is clearly the way to go. Thorough due diligence protects against such over-optimism.

In the pages that follow, we apply this due diligence process to some recurring technical problems with current and proposed identification programs. And we discover—as you'll see toward the end of the report—that ID programs that rely on "shared secrets," such as Social Security numbers or your mother's maiden name, are becoming more insecure due to the increased use of identification. Similarly, ID programs based on biometrics such as fingerprints or iris scans are not the "silver bullets" that some proponents claim they are, but rather could become compromised rapidly if deployed in haphazard ways.

We then apply our progressive principles and due diligence insights to two current examples of identification programs. The first details why it would be bad policy to require government-issued photo ID for in-person voting. The second shows the basically sound policy rationale for the Transportation Worker Identification Card, used for workers with access to security-critical port facilities. By examining one identification program that is reasonable, and one that is not, our analysis shows the usefulness of the Progressive Principles for Identification Systems.

We believe the approach developed in this report favors well-designed identification systems where they are carefully implemented and in the common interest. Design of identification systems should take full account of the Progressive Principles. If that occurs, then the problems of the ID Divide will become far more manageable.

Authentication over Identification

The distinction between "authentication" and "identification" is key to understanding why some ID programs might work and why others clearly won't. As defined by the National Academy of Sciences, authentication means "the process of establishing confidence in the truth of some claim."[1] Identification, in contrast, "is the process of using claimed or observed attributes of an individual to infer who the individual is." In other words, authentication is about being authorized to do something; it can exist without proof of identity. For instance, an ordinary ticket to a movie theater is authentication—the person is allowed into the theater but the person's name is not required. Identification goes a step further. The claim that is being established, or authenticated, is about the person's identity.

There may be situations where both authentication and identification are necessary. Unlike gaining entrance to a movie theater, obtaining a seat on an airplane (given what happened on 9/11) requires that government have sufficient information to determine the identity of the ticketholder and that he or she does not pose a threat to that flight. Other factors, such as your citizenship, may be important if you are flying internationally, but not if you are flying between two cities within the United States. A secure passport is the most appropriate means of conveying citizenship. It is not necessary for a driver's license to do so. In fact (as we explain later in this paper) as more requirements are loaded on any one identifier, the weaker that single ID potentially becomes.

At least two major considerations counsel for the use of authentication rather than identification where feasible. First, experts from diverse parts of the political spectrum have cautioned against the overuse of identification systems. From the point of view of political theory, pervasive identification is a central component of government surveillance. If the use of identification increases substantially, then the data collected by government can at least potentially become a tool for government overreaching.

This point was made by left-of-center participants in our Progressive Identity Project, and is also made, for instance, by Jim Harper of the right-of-center Cato Institute. The central theme of Harper's recent book, "Identity Crisis: How Identification is Overused and Misunderstood," is that identification is overused and should often be replaced with authentication procedures.

The second major consideration is computer security. Modern identification approaches rely much more on an **"ID system"** rather than an **"ID card."** In an ID system, there are often centralized databases and many new flows of personally identifiable infor-

mation, or PII in industry parlance. A centralized system, containing all of a person's data, means that a single data breach can compromise all of that data. A single identifier, such as a Social Security number or fingerprint, can be the key for getting access to all of that data. In everyday terms, consider how dangerous it would be to have a single key for all of your daily uses—your home, car, safe-deposit box, office, and so on. If your employer or anyone else got a copy of that key, they could gain entry to everything else. In the physical world, we would never accept that risk. The single-key aspect of centralized systems thus makes it very difficult to build and operate centralized ID systems in a secure way.

Indeed, the policy, procedural, and technical security challenges are so difficult that the National Academy of Sciences released a book in 2002 entitled: "IDs—Not That Easy; Questions About Nationwide Identity Systems."[2] The analysis in the book, as reinforced by the leading computer security experts who participated in the Progressive Identity project, shows strong reasons to seek authentication where feasible, rather than identification.

The Recent Increase in Amount of Identification

We begin with the increase in the amount of identification required in our society today. In contrast to many other countries, the American tradition has been to avoid a national identity card or system. There was such opposition to the Social Security number when it was introduced in the 1930s that President Roosevelt promised that it would never be used for anything other than Social Security. Yet since then the Social Security number has moved well beyond its original purpose to become a de facto financial identifier. It is broadly required to get a job, open a bank account, or acquire a credit card or mortgage. For a time, there was even crossover where the Social Security number was listed on a driver's license, but states retreated on this as identity theft proliferated.

That realization, and American's continued resistance to a "national ID card," met a new challenge after the 9/11 terrorist attacks, when many looked to new identification systems as part of the overall approach to national and homeland security. Much of the burden has fallen on the driver's license. Because it is the "ID of choice" held by a significant majority of adult citizens, there have been efforts to strengthen its characteristics—notably in the REAL ID Act.

Adding to the complexity of the problem are the sharply increasing amount and variety of identification in the United States in recent years. For instance, ID has been required (or at least strongly suggested) to begin a new job since 1986, to open financial accounts since money laundering laws of the 1980s and 1990s, and to board an airplane since 1988.[3]

Part of the increase in authentication is due to the spread of consumer credit. Lenders usually insist on some form of identification, because they hand out money at the beginning of the relationship and need to know where to go afterward to get repaid. The credit reporting system became truly national about 1970, at the time of the Fair Credit Reporting Act. Credit cards have spread rapidly and continuously since their start in the 1960s. The private sector, therefore, has increas-

ingly developed identification systems as an integral part of modern consumer buying and lending.

Part of the increase in identification is due to new telecommunications and computer technology. As communications speeds rise and costs fall, it is increasingly cost-effective in numerous settings to check back with a central database to verify identity and authorize action. Credit card companies, for instance, instantly double-check new purchases to estimate whether they seem fraudulent. Similarly, modern telecommunications and computers make it feasible for airport security to check passengers against an updated watch list.

On the Internet, the first e-commerce transactions began in 1993, a mere 15 years ago. Online transactions need some form of authentication (although not necessarily identification). The famous cartoon says "On the Internet, nobody knows you are a dog."[4] But online merchants are understandably reluctant to sell to a dog, and the Social Security Administration seriously wants to avoid sending any pension checks to dogs. Emerging technology, therefore, makes it easier to check identity against a database, and more important to authenticate for the myriad activities done online.

Then there's the ID reaction to the 9/11 attacks, another important source of efforts to increase identification. A number of the hijaackers were issued drivers' licenses after providing false documents, drawing attention to weaknesses in the current system of birth certificates and other "breeder" or "foundation" documents for identity systems. More broadly, the emphasis on security since 2001 has led to numerous proposals to require stricter proof of identity in a range of settings, which in turn have led to proposals for more secure forms of identification. Cases in point:

The REAL ID Act of 2005 seeks to require all states to meet detailed federal standards for drivers' licenses and creates interconnected computer access to the data across the states and the federal government. The Act was included in a must-pass Iraq War spending measure, and was never debated in the Senate. Proposed rules for REAL ID were issued in January, 2008 and have been the subject of heated debate. Under the rules, a more secure driver's license, or similar credential, will be required to enter a federal building or for normal access to an airplane.

- Additional security features are being incorporated into the U.S. passport, including a computer chip and digital photograph that at least in theory offer greater protection against fraud. After an extended phase-in period (passports are good for 10 years), U.S. citizens will need an E-Passport, passport card (with a radio frequency ID chip) or enhanced driver's license (which complies with the Western Hemisphere Travel Initiative) to return to the United States from Canada, Mexico or overseas.

- Workers at major U.S. ports are now being issued the Transportation Worker Identification Credential, or TWIC, a biometric identification card for longshoremen, truckers, vessel operators, and other workers, to control access to maritime critical infrastructure considered vital to the U.S. economy.

- On a currently voluntary basis, U.S. employers are being encouraged to use the E-Verify system to match prospective employees and Social Secu-

rity numbers. Arizona, though, now requires employers to participate in the program. While sometimes touted as a security measure, it is primarily intended to prevent immigrants without status from obtaining employment—a distinct issue that has little to do with national or homeland security.

In summary, economic, technological, and policy trends have led to increased amounts of identification and authentication. In recent years, millions of Americans have become increasingly accustomed to showing their drivers' licenses or other IDs in a greatly increasing range of circumstances. This increase in the use of identification is important to understanding the policy issues for current and proposed ID systems. We simply do not have a long-established identification system that is working well. Instead, we are in the midst of a period of rapid change. Signs of strain are apparent already, notably including large increases in identity theft alongside the difficulty or inability of millions of Americans to satisfy the requirements of the increasingly strict requests for identification.

The ID Divide

Much has been written about the "digital divide" that separates Americans with good computer access from millions of Americans who lack access to the Internet. The digital divide is a concern because those who lack access to computers and good Internet connections lose numerous opportunities for education, commerce, and participation in civic and community affairs. The rising prevalence of identification today is creating a similar "ID Divide." For millions of Americans, the recent rise in identification in the United States creates new challenges. IDs are requested in an increasing array of situations, such as getting on an airplane, opening a bank account, starting a job, entering an office building, or voting in elections. These insistent requests for identification detrimentally affect the lives of those who lack ID cards, are victims of identity fraud, or get wrongly placed onto terrorist watch lists or other "high-risk" lists.

The Credentialed and the Uncredentialed

The problems of the ID Divide are invisible to many "credentialed" Americans of the middle or upper-middle class. These Americans include most government employees and policy experts who work on issues of identification. Credentialed Americans take ID checks for granted. Their wallets often contain a dozen forms of identification, all linked to the same name and address. The wallet often holds a driver's license, some credit cards, and membership cards ranging from their employer to an airline to the local grocery store. For these credentialed Americans, showing ID has become second nature. When asked, these credentialed Americans may see little objection to requirements for showing ID to perform tasks in society. For instance, some polling shows that a majority of Americans favors showing ID in order to vote.[5]

The interest-group politics surrounding identification reinforce the views of credentialed Americans. Key decisions about most new identification initiatives happen deep within the government procurement process. Government contractors have a built-in interest in advocating for increased use of identification systems—they get lucrative contracts only if the new systems go forward. Government contractors thus have the economic incentive to be deeply involved in identification proposals at every step of the way.

These ID system vendors also have the economic incentive to develop studies and statistics that support expensive new identification systems. By contrast, public interest groups lack the same staffing and resources to be involved in every state and every

federal agency identification initiative. As a result, even a clear public interest victory in one procurement contract can be ignored in other forums. For instance, the U.S. State Department, after intensive public criticism on security grounds, in 2006 agreed to put physical safeguards around the use of radio-frequency identification chips in U.S. passports. Unfortunately, the State Department and Department of Homeland Security subsequently neglected to use the same safeguards for the "passport cards" and "enhanced driver's licenses" that U.S. citizens are supposed to be able to use at the border in place of full passports.[6]

Credentialed Americans often have not realized what life looks like from the other side of the ID Divide. A major goal of this report is to inform the readers about the size and consequences of the ID Divide. There are at least four categories of problems under the ID Divide:

- **A large population affected by identity theft and data breaches**
- **The growing effects of watch lists**
- **Specific groups that disproportionately lack IDs today**
- **The effects of new and stricter ID and matching requirements**

These problems give reasons for caution about implementing identification systems—the systems often have large, negative effects on those on the other side of the ID Divide. Where systems are indeed implemented, then these problems show the great importance of designing systems with policies to address such problems.

Large population affected by identity theft and data breaches

The ID Divide can strike every American. Identity theft is the fastest-rising crime of the new millennium.[7] The Federal Trade Commission reported that 8.3 million Americans suffered identity theft in 2005,[8] and identity theft is by far the largest category of consumer protection complaints to the government.[9] In a 2003 national telephone survey, 16 percent of adults reported they had been the victim of identity fraud.[10] Identity theft can change any credentialed American into one who faces the insecurities and obstacles facing a person who lacks ID. Identity theft strikes both wealthy and poor Americans, and has happened even to members of Congress.[11]

The rising tide of data breaches increases Americans' vulnerability to identity theft.[12] Recent years have seen innumerable press reports of loss of personally identifiable data from public and private databases. The Privacy Rights Clearinghouse has documented over 226 million data records of U.S. residents that have been exposed due to security breaches since 2005.[13] The TJMaxx clothing stores and affiliated stores lost over 45 million credit and debit card numbers in 2007. The databases of credit card processor CardSystems were hacked in 2005, resulting in loss of data for 40 million Americans. In the public sector, the Veterans Administration lost a data device containing the Social Security numbers and other personal data of 26.5 million discharged veterans. Along with breaches from many other government agencies, there have been repeated reports of computer security problems in federal, state, and local government computer systems.

Most identity programs create centralized databases that are vulnerable to such data breaches. In addition, almost all identity programs create new forms of information sharing, such as when a new employer or motor vehicle bureau checks a name against a central database. These new databases and new information flows are sources of vulnerability, requiring better computer security than has often occurred to date. Especially for official government databases, the new databases can also become targets for organized crime and other groups that seek to commit ID theft on a large scale or gain false credentials for their members. A related problem, discussed further below, is the devastating effect of a breach for fingerprints and other biometric information. When a breach occurs for a credit card, the bank can issue a new card. But once a fingerprint is known, it is very hard indeed to get a new finger.

The more ID checks in society, the more that identity theft matters. In previous decades, with little use of ID checks in America, identity theft was not an important issue. Today and in the future, as ID checks become far more widespread, any imperfections in a person's identity become more serious and likely more difficult to correct. Identity theft today applies to the credit card fraud and bank account takeovers that are perhaps most widely known. Other sorts of identity fraud, moreover, are becoming more common. Medical ID theft has grown, as uninsured people try to get medical care using the name and health insurance of other people.[14] Convicted criminals have a strong incentive to take over an innocent's person identity so that they can present "clean" credentials to be hired, open a financial account, or do other everyday actions in society.

As identity fraud spreads, the victims of fraud may find it difficult or impossible to cleanse records of the false data created by the fraudster. This false data, in turn, increases the likelihood of additional problems for the innocent victim, such as failing a background check, flunking matches with another database (as discussed below), or being placed on a watch list. Identity theft thus can place any American on the uncredentialed side of the ID Divide. A crucial problem in badly designed identification systems is that they can lead to greatly increased rates of identity fraud. Design of identification systems, therefore, should carefully consider how to prevent or mitigate the effects of identity theft.

Growing Effects of Watch Lists

Another way that any American can fall on the wrong side of the ID Divide is to get on a watch list. The No-Fly list operated by the Transportation Safety Administration is expected to expand to over 1 million names in 2008. Problems with this list have become famous. Sen. Ted Kennedy (D-MA) and Rep. John Lewis (D-GA) got on the list. So did Catherine Stevens, the wife of Sen. Ted Stevens (R-AK). Her nickname, "Cat" (as in Cat Stevens, the 1960s folk rock star turned Muslim poet), triggered the scrutiny.[15]

Even these politically prominent individuals have found it very difficult to get removed from the watch list. Even after individuals think they have the problem fixed, they often get placed back onto watch lists, such as when the "evidence" that mistakenly put them on the list in the first instance gets sent into the database again. As with identity theft, a major problem for badly designed identification

systems is that larger numbers of people get flagged as "suspicious," triggering a cascade of problems for individuals as they are asked for ID in daily situations. The problems of identity theft and watch lists already affect many Americans directly. If and as identification systems continue to multiply, they are more likely to affect all Americans at least indirectly because authentication systems create a risk for each individual of losing control over one's identity, with the associated burdens of falling onto the wrong side of the ID Divide.

Specific Groups that Disproportionately Lack IDs Today

Many Americans mistakenly believe that almost all U.S. adults have a driver's license. Over 20 million Americans of voting age currently lack a valid driver's license, however.[16] The Carter-Baker Commission estimated that 12 percent of voting-age Americans lack a driver's license.[17] Lack of a driver's license increasingly affects non-driving aspects of daily life, such as under the new state laws that require a government-issued photo ID in order to vote. Under the REAL ID Act, once implemented, lack of such an ID would prevent access to federal buildings and require additional screening before a person could fly in an airplane. Yet there are, of course, ***driving-related reasons*** why many Americans do not have a driver's license.

- **Blind and other disabled persons.** Roughly 1 million Americans are legally blind.[18] Many Americans have other disabilities that make it difficult or impossible to drive. Persons who cannot drive clearly have less reason to go through the hassle and expense of getting a government-issued photo ID from the motor vehicle bureau. In addition, many blind and disabled people live in poverty.[19]

- **The elderly.** Millions of older Americans no longer drive. Some live in nursing homes or other assisted-living facilities. According to a study by the AARP Georgia chapter, 36 percent of citizens in Georgia over the age of 75 do not have a current driver's license.[20] A Wisconsin study estimated that 23 percent of persons 65 years or older do not have a driver's license.[21]

- **The young.** Teenagers do not automatically get a driver's license when they turn 16. A license may be a costly luxury for cash-strapped families. Many states now require costly drivers' education before issuing a license. Auto insurance rates skyrocket when a teenager is added to the family policy. Some families, especially in urban areas, do not own a car. In addition, college students and other young people move often and so may lack proof of residence. The Wisconsin study found lower rates of licenses for 18-to-24-year-old adults, especially in minority communities.

- **Suspended licenses.** Many states have expanded the range of reasons why driver's licenses are suspended or not renewed. For instance, Oregon has over 100 offenses that can lead to suspension, almost half of which have nothing to do with driving.[22] Massachusetts suspends licenses for failure to pay parking tickets. In Wisconsin, "you can lose your driver's license if you forget to pay your library fines, don't shovel the snow off your sidewalk, or

don't trim a tree that overhangs a neighbor's property."[23]

- **"Driving while poor."** Poor families clearly have a harder time than wealthy families in paying for driver's education, a license, and a car. An additional problem is that poverty can lead to inability to pay traffic tickets or other payments needed to renew a driver's license. According to the Wisconsin study, "The vast majority of suspended licenses in Wisconsin are for failure to pay municipal and circuit court fines and civil forfeitures (sometimes called 'driving while poor')."

- **Urban users of mass transit.** Millions of Americans rely daily on buses, subways, and other forms of mass transit. In an era of dependence on foreign oil and concerns about global warming, this use of mass transit should be encouraged. Yet urban users of mass transit have less reason to get a driver's license, and thus are disproportionately excluded from systems that require one.

- **Lost, stolen, or mutilated driver's license.** Based on available statistics, approximately 20-to-25 percent of operating licenses issued each year are duplicates, issued because the original license was lost, stolen, or mutilated.[24] The time and expense to get a replacement license is manageable for a well-to-do person, or one who needs to show a driver's license for ID checks regularly (such as a frequent airline traveler). In contrast, the expense and hassle of getting a replacement license will be more of an obstacle to low-income people and those who do not need an ID except to vote.

In addition, communities of color and some faith communities are significantly less likely to have government-issued photo IDs, among them:

- **African Americans.** According to a 2006 survey by the Brennan Center, 25 percent of African-American voting-age citizens nationwide have no current government-issued photo ID, compared to 8 percent of white voting-age citizens.[25] In the detailed Wisconsin study, only 47 percent of Milwaukee County African-American adults had a valid driver's license, compared to 85 percent of white adults in the rest of the state. The situation for young adults ages 18-to-24 was even more striking, with 26 percent of African Americans in Milwaukee having a license compared with 71 percent of young white adults in the rest of the state.[26] In a Georgia study, African Americans were 83 percent more likely than whites not to possess the ID, while in Indiana they were 57 percent more likely.[27]

- **Hispanics.** Similar statistics apply to Hispanics. In the Georgia study, Hispanics were twice as likely as whites not to have a government-issued photo ID. In Milwaukee County, Wisconsin, only 43 percent of Hispanic adults had such IDs, and only 34 percent of Hispanics ages 18-to-24 did. In addition, Hispanic citizens born outside of the United States often face significant barriers to obtaining ID, as discussed further below for foreign-born citizens generally.

- **Native Americans.** Although less data exists for Native Americans, the Brennan Center reports that in the five counties in South Dakota with the

highest Native-American populations, voters in the 2004 primary were 2-to-8 times more likely not to bring ID to the polls than other voters in the state.

- **Faith communities.** Some Americans have religious objections to being photographed for government-issued photo IDs. Strict requirements to provide IDs thus can have a serious effect on the Amish and other faith-based communities. Approximately a dozen states have laws on the books with a religious exception to the photograph requirement on driver's licenses, but it appears that these laws may be overruled by the proposed rules for implementing the REAL ID Act.[28]

ID Requirements Exclude Many Eligible Persons

There is clear, recent evidence that the lack of identity documentation has harmful effects in programs where stricter ID is required. The Deficit Reduction Act of 2005, for example, required states to obtain satisfactory documentary evidence of U.S. citizenship or nationality for approximately 40 million Medicaid beneficiaries. The stated goal of the requirement was to prevent noncitizens, who are ineligible for Medicaid, from receiving the medical benefits. A Government Accountability Office study instead found that the major effects of the program were higher administrative costs for the states and denial of medical benefits to eligible U.S. citizens.[29]

Although most states had not quantified the effect of this provision of the Act, the study reported that one state "that had begun tracking the effect identified 18,000 individuals in the 7 months after implementation whose applications were denied or coverage was terminated for inability to provide the necessary documentation, though the state believed most of them to be eligible citizens."[30] Administrative costs and denials of coverage occurred because the documentation requirements lacked exceptions and mandated use only of originals, so individuals had to be processed in person rather than by mail. These higher costs meant that only one of the 44 reporting states experienced savings from the provision, which was designed to save money by screening out ineligible applicants.

This Medicaid experience illustrates the potentially harmful effects of ID requirements on eligible citizens. The effect is more striking because the affected individuals had an important incentive to participate in the program—to receive medical insurance. Where the tangible benefit to individuals is lower, such as getting an ID card in order to meet state voting laws, the exclusionary effects of an ID requirement quite possibly will be higher.

The Effects of New and Stricter Documentation and Matching Requirements

Proposals and programs are currently underway for stricter ID requirements in areas such as voting, employment, driver's licenses, and eligibility for Medicaid and other government programs. The stricter requirements will be costly for many Americans—in terms of time and money to gather documents, and also due to the effects on eligible people who are not able to prove their identity. Recent experience with "matching" programs also highlights the problems that

occur when a large fraction of individuals don't "match" a database due to any of a number of possible causes.

Fees for ID documents: even "free" is not free

States vary in how much they charge for driver's licenses and other state-issued photo IDs. Some states already charge as much as $65.[31] The fee for a license quite possibly will increase substantially in coming years, as states cope with the increased requirements of the Real ID Act without matching funding from the federal government. A U.S. passport costs at least $100 for unexpedited service.[32] For people who drive a car regularly, this level of cost for a driver's license is only part of the overall cost of paying for a car, auto insurance, and the gasoline and other expenses of driving. For people who don't drive, however, these fees are a new tax on their family resources if they are required to get state ID.

These charges by the government, furthermore, are only a fraction of the actual cost to individuals of getting an ID. Original birth certificates are increasingly required by many state agencies. The cost of getting an original birth certificate can be $50, with online services charging additional amounts to deliver them to your home. Some Americans have no birth certificates, including those born at home and those whose town records were washed away in Hurricane Katrina or other natural disasters. For children of the military and other citizens born outside of the U.S., including on now-closed facilities such as Clark Air Force Base in the Philippines or in the Panama Canal Zone, it can be difficult to provide proof of birth. At least 13 million U.S. citizens lack documentary proof of citizenship.[33] Documentation of U.S. citizenship costs over $200, and often takes months to process. In addition, under the REAL ID regulations, individuals will incur additional costs for documentary proof of name changes, such as after marriage, divorce, or adoption. Tens of millions of such individuals will need to have, or pay to get if they don't have, wedding licenses or court documents proving divorce or adoption.

The time and effort of going to the state agency office can be daunting. As Supreme Court Justice Stephen Breyer wrote in his dissent in the recent Supreme Court case about Indiana and voter ID, "an Indiana nondriver, most likely to be poor, elderly, or disabled, will find it difficult and expensive to travel to the Bureau of Motor Vehicles, particularly if he or she resides in one of the many Indiana counties lacking a public transportation system." And that would be the case only if citizens heading for their polling stations to vote know the law is in effect. Just ask those nuns who tried and failed to vote in the May Indiana presidential primary.

In addition, stricter identification requirements can impose multiple burdens. In Colorado, for instance, even a valid passport is no longer sufficient to get a driver's license or a non-driver's state ID. These sorts of burdens are magnified by experience that shows that people lose or misplace millions of driver's licenses and related documents each year. Although wealthy people can easily afford to order another copy, for poorer people loss of an ID creates another round of burdensome time and expense.

States including Indiana and Georgia have responded partially to the concern that requiring a state photo ID to vote

is an unconstitutional "poll tax." In the 1960s, the Supreme Court found a fee of $1.50 to be an unconstitutional poll tax. Adjusted for inflation, any cost over $8.79 today is more than $1.50 at that time. These states have now offered a "free" photo ID for indigent citizens—free in the sense that the state does not charge a fee for the ID.

Problem is, "free" is not really free. Gathering the underlying documents can be expensive, even more so for the millions of Americans who cannot readily produce a U.S. birth certificate. As Justice Breyer notes, the "poor, elderly, and disabled" often face special burdens in getting to state offices and navigating the bureaucracy. In addition, some states will not issue a state ID until a person has caught up on all outstanding payments due the state, including traffic fines and court-ordered child support payments. As ID requirements spread, persons who cannot afford to make all such payments may be denied the right to vote, to receive health insurance, or to become lawfully employed.

The problems of matching programs

A prominent feature of new identification programs is to require "matching" with one or more databases before a person is eligible to participate. Under the Real ID Act, the Social Security number of the applicant is matched against a database of Social Security numbers. Under the Basic Pilot/E-Verify Program, participating employers check name, date of birth, and Social Security number of new hires against a federal database, with a "tentative non-confirmation" notice resulting if the match is not exact. A number of states have proposed or adopted policies under which they refuse to add registrants to the voter rolls unless their voter registration information has been "matched" to information in other government databases, including the state's motor vehicle database or the federal Social Security database.

At first glance, this sort of matching may seem like an easy and common-sense way to reduce fraud and improve the identification process. On closer inspection, however, there is compelling evidence of major problems in current matching programs. Unless matching programs are conducted with high-quality safeguards, often not in place today, they may well increase the number of mistakes in the system. Three categories of errors are prevalent:

- ***Name variation.*** Names used in identification systems are less stable than many would think. Birth certificates (with a maiden name) vary from the married name for tens of millions of Americans. Millions of Americans divorce, with some but not all changing names. Many people use nicknames, their initials, or a middle name. Adopted children often have a name that differs from their birth certificate. For naturalized and native-born citizens, a name given in a foreign language may be spelled in different ways when written in English. Especially for Asian Americans, first and last names are sometimes transposed. In all of these instances, the "name" existing in one database may be different than the "name" for the same person in another database or on another identity document. Depending on the system, identification or eligibility may be refused unless there is iron-clad (and often expensive to get) proof that the earlier name is properly matched to the later name.

- ***Address variation.*** The Real ID Act requires an individual to provide documentary proof of a current, permanent address. For families who have owned a home for years, this proof may be easy to supply. Numerous Americans, however, will have more difficulty defining and proving such an address. For instance, such proof may be difficult for military families, renters, and college students. The requirement of having a permanent address is even more difficult for homeless persons and other transients. The proposed Real ID regulation makes no mention of how to issue ID to homeless persons, although states can likely create an exceptions process if they choose.

- ***Typos, transpositions, and other errors.*** Government and private-sector databases contain far more typos, transpositions (switched digits), and other errors than most people realize. Social Security numbers, unlike credit cards, do not have a "checksum," meaning there is no way to tell from the numbers themselves if an error has been made. The Social Security Administration's Master Death Index, for example, is known to have an error rate of more than 3 percent[34]—yet it is often used to identify voters who are allegedly deceased. Matching records in the health care system, in a so-called Master Patient Index, often results in error rates of at least 5-to-10 percent.[35] These error rates may be less surprising if you imagine re-typing all of the phone numbers and email addresses in your personal address book. High error rates, however, can cause big problems affecting tens of millions of people if a person is denied eligibility due to a single incorrect digit in a database.

  One example is what happened to Bill Cattornini, a 33-year veteran of the Chicago Fire Department. Due to a discrepancy between his birth certificate and his Social Security record, he was unable to renew his driver's license under the new Illinois procedures to implement the Real ID Act.[36]

Errors in matching programs for voting

To promote accuracy in voter rolls, it makes sense to build matching programs that help update voter rolls concerning those who have died or moved away. Unfortunately, many current "matching" processes fall far short of technical best practices, and these policies regularly result in the disenfranchisement of eligible voters through no fault of their own. The Brennan Center has done a major study of problems with voting matches. The number of eligible voters who could be excluded by a "no match, no vote" policy is staggeringly high. One reason for the high rates of "no match" is the large portion of Americans who change residence each year, leading to lack of match on address. Simply purging the rolls, however, would result in large-scale disenfranchisement.[37] Several cases in point:

- A trial run in New York City showed that 20 percent of eligible registrants could have been disenfranchised for reasons including typos by election officials in driver's license numbers.

- In Los Angeles County, almost 20 percent of eligible registrants were excluded from the rolls because of matching problems before the state revised its voter registration policies.

- In Pennsylvania, the number of eligible registrants excluded was as high as 30 percent.

- The Social Security Administration reported that 28.5 percent of the voter registration records checked against its database produced no match. One reason for this high no-match rate is that the agency only finds a "match" if every letter and number is identical to its records. A single typo or other variation (such as use of "Rob" or "Bobby" for "Robert") results in a negative answer.

- African Americans account for 13 percent of Florida's voting-age population, yet were four times more likely than whites to be incorrectly singled out under the state's database matching methodology.

Errors in matching programs for new hires

There have similarly been large-scale problems with matching under the "Basic Pilot" program, now re-named "E-Verify." The program is a voluntary Internet-based program that enables employers to electronically verify workers' employment eligibility by accessing information in databases maintained by the Department of Homeland Security and the Social Security Administration. Approximately 43,000 employers are currently enrolled in Basic Pilot/E-Verify—less than 1 percent of the approximately 6 million employers in the United States—and not all of those enrolled are "active" users.[38] Arizona now requires employers to participate in E-Verify, and there have been proposals to make E-Verify mandatory nationwide.

Both government and independent reviews of the program showed serious problems in the current E-Verify matching program.[39] The Social Security Administration estimates that 12.7 million of its records contain discrepancies related to name, date of birth, or citizenship status for U.S. citizens. If E-Verify were to become mandatory and the databases were not improved, these discrepancies alone would result in 2.5 million people a year being misidentified as not authorized for employment. Foreign-born U.S. citizens feel the greatest impact, with almost 10 percent receiving initial determinations that they are not authorized to work. Additional, serious problems result from the immigration service's consistent history of mishandling the huge volume of data for which it is responsible, evidenced in a GAO review in 2006 that found over 110,000 immigrant records were lost entirely.

In addition to these matching problems, independent reviews of the E-Verify program have found that employers engage in prohibited employment practices, including pre-employment screening, adverse employment action based on tentative non-confirmation notices, and failure to inform workers of their rights under the program.[40] There are also serious concerns about the lack of effective redress mechanisms for individuals whose information does not match.

Still, some progressives see the value of a well-designed employment verification system, especially if it is part of comprehensive immigration reform. But consistent with the Progressive Principles for Identification set forth in this Report, an expanded E-Verify program should proceed only if and when it passes the due diligence test, achieving important goals

while effectively addressing the accuracy and other problems that have troubled the system to date.

Errors in matching programs for driver's licenses

There have been significant problems for states that have begun to implement the name- and address-matching requirements in the Real ID Act. Perhaps the most telling case is in Alabama:

"One of the Real ID Act's requirements is that names on compliant driver's licenses must exactly match individuals' names as held by the Social Security Administration. Noting this, officials in Alabama decided to get a head start on complying with that aspect of the law. The state's motor vehicles department (the Department of Public Safety or DPS), began sending letters to individuals whose records were mismatched, demanding that they correct the "erroneous" information on their driver's licenses.

The result was a fiasco. Thousands of panicked Alabama residents jammed DPS offices worried that they would lose their right to drive. And, because the state began its records review with the oldest records, many of the reported 65,000-80,000 drivers who got letters were senior citizens."

Many recipients of the letter—some of whom had been driving for 50 years or longer—became panicked that they would lose their means of traveling around the largely rural state. Many elderly drivers were also reportedly worried that their Social Security checks or pensions would be interrupted if they did not 'fix' the problem right away. 'Here are people who have been law-abiding citizens all their lives, and then they get this letter,' state legislator Neal Morrison told the Associated Press. "It scared them to death.'"[41]

Although Alabama pulled back its program in order to change it, similar problems have recently occurred in Indiana. The Indianapolis Star reported in November, 2007: "Beginning next week, the Bureau of Motor Vehicles will send letters to 206,000 people asking them to update their driver's license or state identification card information. If the BMV doesn't get correct information or does not hear from those people, their licenses or ID cards will be revoked."[42]

Summary on the ID Divide

The rapid increase in the use of identification in American society has been accompanied by the growing problem of the ID Divide. Identity theft and watch lists can place any American on the wrong side of the ID Divide. In addition, far more adult American citizens lack a government-issued photo ID than most people realize. And matching programs in voting, employment, and driver's licenses currently fall far short of technical best practices and have shown deeply problematic effects of excluding many eligible citizens and residents.

Although Americans of all backgrounds may find themselves on the wrong side of the ID Divide, there are disproportionate effects on the poor, the young, the disabled, the less-educated, communities of color, and citizens born outside of the United States. For a credentialed, middle-class family that has the same home and jobs for years, it may be relatively easy to provide documentation and to rectify

problems if they occur by producing multiple other documents. Such families may also be more skilled at navigating the bureaucracy than the less-educated, those who are less fluent in English, or those who can't afford to take off multiple days from work to satisfy the demands of the motor vehicles office. Because most legislators and policymakers are themselves thoroughly credentialed, it is especially important for them to learn about the daunting challenges facing the uncredentialed.

In recent years, debates in the United States about identification have been dominated by the goals of fighting terrorism or addressing immigration issues. As our country considers expensive identification systems, which are designed to last for many years, it is vital to consider the effects of new programs on all citizens and legal residents. The price of fighting terrorism should not be to exclude millions of law-abiding Americans from participation in society.

New Haven Pioneers New ID Program

Connecticut city issues city ID cards with punch

In response to the ID Divide, some jurisdictions have experimented with ID cards that lessen the squeeze on those who lack a passport or driver's license. The program in New Haven, Connecticut is one such example. Local residents can bring proof of residency to city officials and be issued a city ID card for $10. Fraudulent identity documents are screened out, but people lacking "foundation" documents are assisted in how to get proof of identity.

To encourage residents to get a card, the new ID can be used for many purposes, including: library card; debit card; coinless alternative for parking meters and garages; access to the beach and other city facilities; getting free flu shots; recycling; and to open a bank account. The state attorney general has certified that the card satisfies ID requirements for voting. Police officials have testified that the program reduces crime, because otherwise-undocumented residents are more willing to cooperate with the police when they have a residency card.[43] One part of the program provides similar ID cards for children.

This New Haven example shows how part of a desirable approach to authentication is inclusion—facilitating a wider range of people participating in civic and economic life. This sort of inclusion benefits both the individuals directly and the community that gains from their participation. Specific instances of inclusion have been politically controversial. For instance, some have advocated issuing state driver's licenses to adults without requiring proof of lawful U.S. residence. Proponents point out advantages such as public safety (more people will drive only after passing a driving test) and lower insurance prices (more people will get the mandatory car insurance that accompanies having a driver's license).

In contrast, opponents have criticized programs that give the state's imprimatur to persons lacking lawful residence status. Our goal in this report is not to recommend a particular solution to this driver's license debate. Instead, a more fundamental point is that inclusion is a significant goal of authentication and identification systems—bringing people into the system reduces the ID Divide, facilitating their lives and including them in communities.

A related point is that authentication without identification may be a way to foster inclusion. For online purchases, for instance, some online payment and new software approaches enable fraud-resistant commerce without the seller needing to know the buyer's identity.[44] In that way, buyers do not have to trust the seller with their personally identifying information.

Due Diligence for Authentication Systems

Key Technical Issues

The need for a "due diligence" process when considering and implementing identification systems is key to coping with the ID Divide. The term "due diligence" is used in mergers and acquisitions and other important corporate transactions to describe the careful vetting before a company makes a major investment. Proponents of a merger (or in our case at hand, of a new identification program) can err on the side of optimism, concluding too readily that the benefits of a merger (or an ID or other security program) will demonstrably improve the situation. In response, a due diligence process looks for the characteristic ways that things might go wrong.

Performing due diligence on new identification programs before implementing them, based on our six progressive ID principles (see page 2) will be critical to any effort to deal with problems of identification and authentication going forward.[45] A similar process should be used to review existing programs, and such a review may well be appropriate for the next administration, which will be headed by the first new president since the events of September 11, 2001. Initial aspects of due diligence include:

- Does the new program actually improve security?
- Does it do so cost-effectively?

If a proposed program cannot pass these initial tests, then there is no need even to consider trade-offs with other important considerations, such as personal privacy, civil liberties, or the right to vote.

After considerable research into the technical and computer security aspects of authentication and identification, we believe that many current approaches have serious risks from a security point of view, and these failures are likely to become more acute over time. This report delves into two of the most important flaws in current approaches—"shared secrets" and biometric forms of identification—which are not widely understood by policymakers. "Shared secret" approaches to identification, such as using a mother's maiden name or Social Security number, are rapidly becoming less effective. And upon closer inspection, the limitations of biometrics, such as fingerprints or iris scans, are far from the "silver bullet" for identification that many have hoped.

Many current and proposed identification systems depend on shared secrets, biometrics, or both, at the core of their systems. Because of important technical problems discussed directly below, weak implementation of these approaches may actually increase identity fraud, and its associated costs and problems, in coming years. Many current approaches

thus appear to be deeply flawed. It is bad policy to spend enormous sums of money on systems that have known large flaws before they are even implemented.

Instead, we should move along a path toward authentication and identification systems that are robust over time. In coming years, we believe that state-of-the-art techniques for online authentication will merge with state-of-the-art techniques for in-person authentication. One long-term trend will be to use devices, such as cell phones or Personal Digital Assistants, which can provide much stricter security and privacy. We now turn to key technical issues that apply to many current and proposed identification approaches.

From "Shared Secrets" to Device-Based Authentication

Most of us are familiar with the use of a "shared secret."[46] We are asked to verify our identity by telling a "secret" that the other party knows as well, such as mother's maiden name or Social Security number. This kind of shared secret is rapidly becoming a weaker and weaker form of authentication, for at least two main reasons. First, modern search engines are excellent at revealing secrets. Second, the increasing use of authentication runs into a brick wall—the more you use secrets, the less secret they become.

It is easy for us to forget how quickly effective search engines have become part of our daily life. Google was only founded in 1999. This means that generations of identity systems were devised before ordinary people could do effective searches about secret facts. Consider the use of a "secret" such as mother's maiden name. Maiden names simply don't stay secret to online genealogy researchers. Today, a moment's search online will reveal articles such as "Top 10 Places to Find Maiden Names."[47]

Similarly, the Social Security numbers of millions of Americans appear online in mortgage deeds, marriage records, and numerous other locations. Many of the "secrets" about an individual that will be available to a corporation or government agency will also be available online to a fraudster seeking that same information.

A more fundamental problem is that secrets degrade the more you use them. Think about how many organizations today have the Social Security number for a typical individual. The Social Security Administration, tax agencies, tax preparers, and every employer in the person's life are only the start. Credit histories are linked to Social Security numbers, so lenders, landlords, phone companies, and insurance companies all have them ready at hand. Many medical records are filed by Social Security number, as are many school records. As already mentioned, many public records for years have included them. At most, someone who wants to learn the "secret" Social Security Number of someone need only find one employee in any of those organizations who is willing to reveal it or who can be tricked or bribed into revealing it.

Benjamin Franklin said: "Three may keep a Secret, if two of them are dead." Americans today are asked for ID far more often than in the past, by many more types of organizations. Anything that is a "secret" known to all of those organizations will simply not remain a secret against a determined attacker.

One particularly important vulnerability is any information that is readable from an identity card. Increasingly, organiza-

tions are making copies of everything on such cards, including photos, fingerprints, and driver's license numbers. This sort of "skimming" is currently lawful, and there are no laws that prevent the ones doing the skimming from disclosing or reselling that information to others. The skimmed information may seem "secret" for at least a little while, and will be taken by people as proof of identity. Over time, however, everyone will realize that the information readable from an ID card is basically public information—all of those copies will mean that the information can no longer be considered "secret." As discussed below in connection with biometrics, placing fingerprints on identity cards, over time, will mean that most people's fingerprints will be easily faked.

Biometrics Are Not a Silver Bullet for Identification

Many persons hope that biometrics can be the "silver bullet" in the future for authentication. The term "biometric" means something that measures your biology, such as a photo, fingerprint, iris scan, or DNA sample.

The attraction of biometrics, at least at first glance, is that they can uniquely identify an individual. There is a glorious simplicity to the idea that an individual can present part of his or her body, and then magically the system responds "yes" or "no" to the person. In this optimistic view about biometrics, people no longer have to worry about remembering passwords or losing a smart card. Instead, individuals simply show up, swipe their finger, and get the desired access.

In our view, biometrics do indeed have potentially valuable uses going forward. They emphatically are not, however, a "silver bullet" for government-issued ID, for at least three major reasons:

- Biometrics do not work or work less effectively for some people and subpopulations, leading to many false positives and negatives
- Biometrics, such as fingerprints, become a "shared secret" and thus insecure over time
- Biometrics, used at the periphery by millions of readers, don't solve the many problems of accuracy and fraud in core databases

Biometrics don't work or work less effectively for some people and subpopulations

Biometric systems, in practice, suffer from two related problems—they don't work as well for some people and subpopulations, and they result in practice in many false positives and negatives. At a minimum, these problems mean that there need to be exceptions procedures, which make an identification system harder and more expensive to deploy.

The problems of fingerprints have been extensively studied.[48] They obviously don't work for people who have lost fingers or hands. They don't work well for children, because of changes in patterns as children grow. They also don't work as well as people age, especially for those over the age of 50.[49] A little-known fact is that fingerprints don't work well for some occupations, including bricklayers, where hard work rubs off fingerprint ridges over time.

A related problem is that problems of inaccuracy rise sharply as the population in the database increases. For instance, if

a system such as airport screening tries to reduce the number of false negatives to close to zero, then it will generate a huge number of false positives. These false positives will then have to go through additional screening, perhaps suffer delays in travel, and there should then be effective redress procedures for those who are inappropriately detained. In contrast, if the screening system tries to avoid false positives, then the result will be a much larger number of false negatives—the suspects will have a better chance to slip through the system.

Shared secrets and the loss of use of biometrics

A crucial, long-term problem for biometrics is that once they are in digital form, they can be copied and sent around the Internet. A fingerprint or other biometric thus suffers from the problems of "shared secrets," discussed above. Computer scientist Terrence Boult has dubbed this problem the "biometric dilemma," which he defines as the more we use biometrics the more likely they will be compromised and hence become useless for security.[50]

The problem is easy to see if one considers proposals to put fingerprints on ID cards. Today, ID cards are increasingly copied by building guards, by bars to prove that someone is old enough to drink, and by many other organizations. Those copies mean that each bar or building guard becomes a possible security leak. Once one clear picture of the fingerprint exists, copies of the fingerprint can be distributed anywhere, including to identity thieves or posted to the Internet.

For fingerprints, a quick online search for "fake fingerprints" will show how to make an effective fake fingerprint. As discussed by noted security expert Bruce Schneier, one technique is available for under $10. It was tried "against eleven commercially available fingerprint biometric systems, and was able to reliably fool all of them."[51] In brief, the digital image is sent to a laser printer. It is then easily transferred to a gel that covers the imposter's finger. That sort of simple trick works for in-person authentication. For online authentication, the picture of the finger is just as accurate as the real finger, so fake remote authentication would be at least as easy.

Essentially, the problem for fingerprints is identical to what has happened for Social Security numbers, which initially were a fairly useful "secret" because only a limited number of organizations had access to the number. Over time, however, many more organizations got access to the numbers, as did identity thieves. Today, Social Security numbers are no longer a secure way to identify anyone. Tomorrow, if digital pictures of fingerprints become similarly widespread, fingerprints will be roughly as easy to fake as Social Security numbers. It is difficult enough, today, for an individual to get a new Social Security number. Getting a new finger will be even harder, to say the least.

Biometrics are only as good as the back-end databases

The other reason that biometrics are not a silver bullet is that the system is only as good as the back-end databases. Suppose, contrary to real-life experience, that a biometric was available that worked for the entire population, avoided false positives and negatives, and was impossible to fake the way that fingerprints can be faked. Even then, a biometric system would suffer serious vulnerabilities.

Notably, the wrong name could be entered into the database connected to the biometric. For instance, an identity thief named Joe could trick the system into having his biometrics entered into the database with a wrong name, such as Jon. Or, the name could be entered incorrectly by mistake ("Joe" and "Jon" are only one letter apart). Or either insiders or outside hackers could alter the database that linked names and biometrics.

These sorts of database problems are common. The many reported data breaches, including by the Veterans Administration and other government agencies, provide the information that fraudsters need in order to pretend to be other people. The proposed REAL ID rules add to this problem by requiring access to records by all 50 states without providing a strong structure for computer security. In brief, even a (utopian) perfect biometric system would be vulnerable in practice to problems in the databases that held the names and biometrics.

Deep Flaws of the Current System

The problems with shared secrets and biometrics help show why many current and proposed identification systems, based on ID cards and centralized databases, are deeply flawed in an era of pervasive identification checks. First of all, shared secrets don't stay secret in our era of search engines and pervasive identification. Second, the problem of shared secrets is made much worse by the bad incentives of those who hold the "secret," identifying data.

The problem arises because the holder of the information only guards the information at the level of risk to that organization. If that information is lost or stolen, there is typically little harm to the data holder. There is a much greater risk of harm, though, for the individual whose information is compromised. As identity information is checked for numerous daily events, there will inevitably be many breaches of the supposedly "secret" data. We have already seen data breaches affecting a majority of Americans.[52]

Third, biometrics do not solve the shared secret problem. Notably, fingerprints could quickly reprise the failures of relying on the Social Security number. "Raw" biometrics— fingerprints and other biometrics that are stored in unencrypted form—are a major security risk. Once the picture or standard template of a fingerprint leaks, other people can readily impersonate that individual on fingerprint readers. To the extent biometrics are used, public policy should strongly encourage the fingerprints or other biometrics to be stored and transmitted in encrypted form. In addition, unencrypted fingerprints should not be included in ID cards. If they are, then it is an open invitation for anyone who checks the card to make a high-quality copy that can be used in the future for identity fraud.

Fourth, centralized databases become a single source of failure. This point was vividly illustrated in early 2008, when the British National Health Service lost a single copy of the records of a majority of the country's children, including their health identification numbers. The security risks associated with centralized databases have led numerous technical experts to emphasize the need for more decentralized authentication systems.[53]

Fifth, any database that scales to 300 million Americans, and over 200 million drivers, will be difficult or impossible to

protect against determined bad actors. An authentication system should be designed to achieve equality and fairness, and to have effective redress mechanisms. Otherwise, parts of the population suffer uncompensated and often substantial burdens. At the same time, however, such a system contains many people who lose documents, change residence often, and have other attributes that are not one-size-fits-all. Determined bad actors will probe for any weak points in the system, and will inevitably find them. When they do get fake credentials, moreover, they may be treated as "gold plated" credentials which give the bad actor dangerously broad access.

Toward a Long-term Solution

Authentication of various sorts is required to do online activities ranging from logging into an employer's system to accessing an online banking account to applying for government benefits. It is interesting, therefore, to examine the six principles of the Authentication Privacy Principles Working Group,[54] a coalition of expert public interest and industry groups at the cutting edge of authentication technologies:

- ***Provide User Control***. The informed consent of the individual should be obtained before information is used for enrollment, authentication, and any subsequent uses.

- ***Support a Diversity of Services***. Individuals should have a choice of authentication tools and providers in the marketplace. While convenient authentication mechanisms should be available, privacy is put at risk if individuals are forced to use one single identifier for various purposes.

- ***Use Individual Authentication Only When Appropriate***. Authentication systems should be designed to authenticate individuals by use of identity only when such information is needed to complete the transaction. Individual identity need not and should not be a part of all forms of authentication.

- ***Provide Notice***. Individuals should be provided with a clear statement about the collection and use of information upon which to make informed decisions.

- ***Minimize Collection and Storage***. Institutions deploying or using authentication systems should collect only the information necessary to complete the intended authentication function.

- ***Provide Accountability***. Authentication providers should be able to verify that they are complying with applicable privacy practices.

These principles support decentralized approaches to authentication, where the data collected is minimized, and the individual is specifically identified only when appropriate. These principles are deeply different in tone and approach from many of the centralized identification systems that have been proposed in recent years.

These authentication principles were based, in large measure, on an appreciation of the security and privacy flaws in centralized systems. The "secrets" on an ID card, checked constantly against a central database, simply will not stay secret for long. Instead, the principles push toward individuals having a separate credential for each part of life, much as individuals today have separate keys

for their home, car, and office. In that way, loss of one key does not leave the individual exposed in all facets of life.

In addition, The National Academy of Sciences, in a major study on authentication and privacy, set forth criteria for an identifier selected for an authentication system:

- Be unique to the system (possibly random)
- Not be widely used
- Not be sensitive or revealing
- Require little or no physical contact
- Entail obvious (as opposed to covert) collection/assignment
- Not be related to communications activities[55]

Although these criteria may appear daunting to put into practice, there is a promising approach that is rapidly becoming far more workable. For people with ready access to a computerized device, the device can use strong, unique passwords for each person for each organization. Fortunately, that kind of device is well on its way to being adopted. It is called the cell phone. Cell phones, laptop computers, smart cards, and other devices increasingly will be usable by ordinary people to provide strong passwords for each organization.[56] There will be a social learning curve about how to do this sort of authentication. Device-based authentication, however, provides a way for individuals to be more secure and to manage what to reveal to organizations asking for proof of identity.[57]

Applying Progressive Identification Principles

Voting and the Transportation Worker Identification Card Program

We now apply the Progressive Principles for Identification to two current examples of identification programs. First, the report explains why it is a bad idea to require government-issued photo ID for in-person voting. Next, it shows the basically sound policy rationale for the Transportation Worker Identification Card, or TWIC program, used for workers with access to security-critical port facilities. By examining one identification approach that is reasonable, and one that is not, the analysis here shows the usefulness of the Progressive Principles for Identification.

Mandatory Photo ID for In-Person Voting

An area of intense current debate is whether government-issued photo ID should be required for in-person voting. Although other methods for identifying voters have long been in place, the first such requirements in U.S. history were passed by Indiana, Georgia, and Missouri beginning in 2002.[58] In May, 2008, the U.S. Supreme Court held 6-to-3 that the Indiana law was constitutional on its face in *Crawford v. Marion County Election Board*.

A law can be constitutional but a very bad idea. For instance, a 90 percent income tax is constitutional, but many people would oppose such a measure. The same applies to mandatory photo ID. When measured against this report's principles for identification systems, mandatory photo ID is a bad policy choice that should not be adopted by the states. A due diligence review shows that requiring state-issued photo ID to vote badly flunks our six progressive identification principles.

Achieve real security or other goals

Proponents of required photo identification say that it will reduce in-person voter fraud, because only those carrying an unexpired state-issued photo ID will be allowed to vote. There have been comprehensive refutations, however, of the claim that photo ID will reduce voter fraud.[59] The most thorough academic examination of the issue is by George Washington University law professor Spencer Overton, in a 2006 *Michigan Law Review* article.[60] Professor Overton examines the leading anecdotes that purportedly show voter fraud, and concludes: "While anecdotes about fraud are rhetorically persuasive, the narratives often contain false information, omit critical facts, or focus on wrongdoing that a photo-identification requirement would not prevent."[61]

Despite an intensive effort by a conservative group to highlight incidents of in-person voting fraud, there were zero confirmed incidents of voter fraud at the polling place in the 2006 elections.[62] Under President George W. Bush, there was a major effort to identity and prosecute cases of in-person voter fraud. A significant reason for the controversial firings of several U.S. attorneys was that they did not prosecute as many such cases as the Justice Department leaders wished.[63] This pressure to find cases resulted in more than 180 investigations into election fraud since October 2002, with charges against 89 individuals and 52 convictions for a range of offenses, including alleged vote buying, attempting to jam phone lines of get-out-the-vote operations, and one case of ballotbox stuffing by an election judge. Despite this effort, "none of the charged instances of election fraud involves an allegation that a voter attempted to impersonate someone else at the polls."[64] The Brennan Center examined each allegation of voter fraud mentioned in any of the briefs in the Indiana case, and concluded that "the briefs cite one attempt at impersonation that was thwarted without a photo ID requirement, and nine unresolved cases where impersonation fraud at the polls was suspected but not proven."[65]

Due diligence for proposed identification systems would ask whether the program achieves the security goal and whether it does so cost-effectively. The academic studies show serious reasons to doubt that a photo ID requirement will reduce voter fraud because of the lack of evidence of the type of voter fraud that would be prevented by the ID. In addition, the cost-effectiveness calculus tilts strongly against having the photo ID requirement. An intensive study of 2.8 million Washington state votes in 2004 found that 0.0009 percent of the ballots involved double voting or voting in the name of deceased individuals.[66] Professor Overton calculates that this rate of fraud, when compared with the over 20 million Americans who lack a driver's license, would mean that "photo-identification requirements would deter over 6,700 legitimate votes for every single fraudulent vote prevented."[67]

From a system security perspective, photo ID requirements target an especially unlikely method of voter fraud. The photo ID requirement targets one-at-a-time votes by people who are willing to commit fraud in the full light of day, examined by poll watchers of the various parties, in the community where they claim to reside. That kind of in-person fraud is riskier and less likely to swing an election than two other categories of fraud—absentee ballots and voting machine fraud.

Absentee ballot fraud, done literally out of sight of voting officials, is less risky for a fraudster than going to the polls, yet states such as Indiana and Georgia allow such voting without any photo ID. Machine-based fraud, such as old-fashioned ballot box stuffing or state-of-the-art hacking of software, has a much higher payoff for fraud because many votes can be stolen at once. In short, moving forward with a photo ID requirement while not addressing other more substantial sources of fraud is not a rational strategy if the goal is truly to reduce voter fraud. This lack of a rational basis for the photo ID requirement is one reason that many observers believe that support for the photo ID is based on partisan political calculations rather than an actual effort to reduce voter fraud.

Accuracy

Accuracy is not a major issue in the debate over whether a photo ID should be required for in-person voting. Accuracy is a major issue, however, when matching programs are used to purge data rolls. As discussed above, experiments have found error rates of 20 percent to 30 percent in programs designed to purge rolls, so great care is required before people are removed from eligibility to vote.

Inclusion

Inclusion is a major reason to be skeptical of proposals for mandatory photo ID for voting. The facts of the ID Divide demonstrate the many millions of citizens who could be excluded from the right to vote—the fundamental basis for democracy—by overly strict ID requirements. As Professor Overton writes: "While a small amount of voter fraud hypothetically could determine a close election, the exclusion of twenty million Americans who lack photo identification could erroneously skew a larger number of elections."

The principle of inclusion underscores the desirability of anti-fraud procedures that are less exclusionary than a mandatory photo ID. For instance, many states have long permitted an affirmation of identity, on penalty of perjury. States often match signatures to the signature at time of registration. Utility bills, bank statements, and other proofs of identity are unlikely to be in the hands of fraudsters. In short, identification approaches can be designed to address fraud while avoiding disenfranchising eligible voters.

Fairness and equality

A major reason for concern about photo ID proposals is the known disproportionate harm to specific groups, including African Americans, Hispanics, the blind, and other groups such as the disabled, the poor, the young, and the elderly. Especially in light of the long American history of discrimination in voting rights, any proposal that has known negative effects on such groups should be done only based upon compelling evidence of need, which is lacking for photo ID proposals.

Effective redress mechanisms

An important and effective redress mechanism is to have back-up forms of identification in addition to government-issued photo ID. The ability of the citizen to sign an affidavit or present more readily available documentation such as a utility bill would greatly mitigate the exclusionary effects of mandatory photo ID approaches. For matching programs, an important principle is to ensure that there is effective notice to any voter before a name is purged from the roles, as well as realistic and effective ways for individuals to vote where the purging is done inaccurately.

Equitable funding mechanisms

ID requirements are done at the state level, so there is no problem of unfunded federal mandates. Matching programs, however, can easily raise the twin problem of unfunded mandates and technology or procedures that have a high error rate. In light of the high error rates in voting matching found by the Brennan

Center, extreme caution is needed before assuming that the infrastructure and staffing are in place to avoid purging eligible voters from the rolls.

Conclusion on Mandatory Photo ID for Voting

Following this report's principles for identification, and based on the actual evidence about voter fraud, requiring photo ID for in-person voting would have significant harmful effects. The recent Supreme Court case may find such a requirement constitutional, but the approach is nonetheless clearly bad policy that should not be enacted. If enacted by states, then necessary safeguards should be put in place to eliminate exclusionary effects.

Transportation Worker Identification Card

The Transportation Worker Identification Card is an example of a current identification initiative that, despite significant flaws, responds to important security concerns. TWIC was created by 2002 and 2006 statutes designed to improve port security. According to the Transportation Security Administration, the "Program's objective is to design and implement a standardized secure credential for the identification of transportation workers whose duties require unescorted physical access to secured areas of the nation's transportation system."[68] Applicants for a TWIC, such as merchant mariners and port facility employees, provide their fingerprints and detailed personal information. The Transportation Security Administration performs a security threat assessment, including review of criminal, immigration, and pertinent intelligence records. Holders of a TWIC reapply after five years, and are subject to a new threat assessment. A due diligence application of our six progressive identification principles demonstrates the TWIC program is a reasonable response to security risks, although modifications are needed to improve the program's fit with our stated principles.

Achieve real security or other goals

The strong rationale for TWIC is that port security should be a priority in the overall assurance of homeland security.[69] Having unsecured access to port areas can lead to the importation and distribution of weapons of mass destruction. It is imprudent to allow such access to known security risks.

As for the questions of whether the program is effective or cost-effective, a key consideration is the extent to which the security threat assessment is a good predictor of risk. Because the program applies only to individuals who have unescorted physical access to secured areas, there is an initial tailoring of the scope of the system to the risk. As discussed under fairness, however, amendments may make the security assessment a better predictor of risk.

In terms of due diligence, the TWIC program was subjected to a detailed privacy impact assessment.[70] A substantial array of technical and administrative measures is in place to safeguard the privacy of applicants' information. For instance, fingerprints are stored and transmitted in encrypted form. In addition, the use of the TWIC for a clearly-defined purpose, rather than as a

society-wide credential, reduces many of the risks of fingerprints or other "shared secrets" being compromised.

Accuracy

The security threat assessment is based on a review of criminal, immigration, and intelligence records. It is unclear how often the Transportation Security Administration will have mismatches, such as where an applicant with a clean record is turned down for a TWIC. Once the program is fully implemented, it makes sense to study carefully the rates of false positives and false negatives.

Inclusion

There are ongoing criticisms of TWIC that the security threat assessment will be applied in an overly mechanistic way to exclude individuals who do not actually pose a security risk.[71] As the program is fully implemented, study is appropriate to examine how well the existing threat assessments and appeals procedures work in practice.[72]

Fairness and equality

One fairness concern is the cost of the credential, which is $132.50 every five years plus the cost to obtain birth certificates and other foundation documents. These costs, and the low wages paid to many of the workers who would need the credential, led the International Brotherhood of Teamsters to recommend that the government or employers should pay for the TWIC as part of the overall effort to assure homeland security.[73]

Effective redress mechanisms

As mentioned in connection with inclusion, there are concerns that individuals will be excluded when they do not pose an actual security threat. Better appeals mechanisms should be developed over time to address these concerns.

Equitable funding mechanisms

Individual workers have to shoulder the substantial costs of receiving a TWIC. The ports themselves bear the lion's share of the cost of installing the card readers and other infrastructure. Because the benefits to homeland security inure to the nation as a whole, it may be preferable for the government, facility operator, or employer to fund a larger portion of the costs of TWIC.

Summary on TWIC

Because the TWIC program is tailored to the specific risks to port security, there is a solid case for proceeding with this identification program. There are important concerns about inclusion, fairness, redress, and funding, however, and there is thus room for improvement in how the program is implemented. There should also be ongoing study of how the privacy and other safeguards hold up under field conditions.

Conclusion

The rising quantity of identification systems, identity theft, and watch lists all are contributing to a newly important ID Divide in the United States. For passports and other purposes it makes sense to have identification systems, run by or on behalf of the government. A major finding of this report, however, is that new and existing identification systems should be subject to due diligence. Systems created in the name of security should only be implemented if they actually will improve security, and do so cost-effectively. The shared secret and biometric discussions beginning on page 21 show the sorts of security risks that are inherent in many current or proposed identification systems. In many instances, it is desirable to seek authentication approaches that do not rely on identification.

A progressive approach to identity and authentication means that the systems should be developed in the common interest, and not primarily for the convenience or ease-of-use of those operating the systems. The actual effects of the ID Divide on ordinary people are a crucial factor in assessing the overall desirability of proposed systems. For that reason, we are recommending that proposed and existing systems be measured against the following principles:

- Achieve real security or other goals
- Accuracy
- Inclusion
- Fairness/equality
- Effective redress mechanisms
- Equitable funding mechanisms

This approach favors well-designed identification systems when they are in the common interest. A due diligence process should prevent proponents from assuming benefits, such as low cost and perfectly working biometrics, that will not pan out in practice. We can move forward as well on authentication approaches that do not rely on identification, and on long-run approaches that rely on cell phones and other devices having stronger security and privacy qualities. In short, there are measures to address the ID Divide. We hope this report can assist the next administration in finding ways to do so.

Glossary

Definitions are from Computer Science and Telecommunications Board, National Research Council, *Who Goes There? Authentication Through the Lens of Privacy* (Washington, DC: National Academy Press, 2003).

Attribute Authentication. Attribute authentication is the process of establishing an understood level of confidence that an attribute applies to a specific individual.

Attribute. An attribute describes a property associated with an individual.

Authentication. Authentication is the process of establishing confidence in the truth of some claim.

Authenticator. An authenticator is evidence that is presented to support the authentication of a claim. It increases confidence in the truth of the claim.

Authorization. Authorization is the process of deciding what an individual ought to be allowed to do.

Biometrics. Biometrics is the automatic identification or identity verification of individuals on the basis of behavioral or physiological characteristics.

Credential. Credentials are objects that are verified when presented to the verifier in an authentication transaction. Credentials may be bound in some way to the individual to whom they were issued, or they may be bearer credentials. The former are necessary for identification, while the latter may be acceptable for some forms of authorization.

Identification. Identification is the process of using claimed or observed attributes of an individual to infer who the individual is.

Identifier. An identifier points to an individual. An identifier could be a name, a serial number, or some other pointer to the entity being identified.

Identity Authentication. Identity authentication is the process of establishing an understood level of confidence that an identifier refers to an identity. It may or may not be possible to link the authenticated identity to an individual.

Identity. The identity of X is the set of information about an individual X, which is associated with that individual in a particular identity system Y. However, Y is not always named explicitly.

Individual Authentication. Individual authentication is the process of establishing an understood level of confidence that an identifier refers to a specific individual.

Appendix: Participants in the Progressive Identity Project

The Progressive Identity Project was chaired by Cassandra Butts, Senior Vice President for Domestic Policy at the Center for American Progress. The reporter for the project was Peter Swire, Senior Fellow at the Center for American Progress and the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University.

The following persons participated in at least one of the in-person meetings of the Progressive Identity Project. They have given permission to be listed as participants, but were not asked to endorse the report itself.

Mr. Mark Agrast
Senior Fellow
Center for American Progress

Mr. Rand Beers
Executive Director
National Security Network

Ms. Cassandra Butts
Senior Vice President for Domestic Policy
Center for American Progress

Ms. Vanessa Cárdenas,
Director, Ethnic Media
Center for American Progress

Ms. Sophia Cope
Plesser Fellow
Center for Democracy and Technology

Mr. P.J. Crowley
Senior Fellow
Center for American Progress

Dr. Carol Diamond
Managing Director, Health Program
Markle Foundation

Ms. Maria Echaveste
Senior Fellow
Center for American Progress

Ms. Julie Fernandes
Principal
Raben Group

Ms. Joan Friedland
Immigration Policy Director
National Immigration Law Center

Ms. Daniella Leger
Vice President of Communications
Center for American Progress

Ms. Kica Matos
Deputy Mayor
City of New Haven

Ms. Tyler Moran
Employment Policy Director
National Immigration Law Center

Mr. Dan Restrepo
Director, The Americas Project
Center for American Progress

Mr. Bruce Schneier
Founder and CTO
BT Counterpane

Mr. Ari Schwartz
Deputy Director
Center for Democracy and Technology

Mr. Michael Signer
Senior Policy Advisor and
Director of the Homeland Security
Presidential Transition Initiative
Center for American Progress

Mr. Tim Sparapani
Senior Legislative Council
American Civil Liberties Union

Mr. Barry Steinhardt
Director, Technology and Liberty Program
American Civil Liberties Union

Mr. Peter Swire
Senior Fellow
Center for American Progress

C. William O'Neill Professor of Law
Moritz College of Law
The Ohio State University

Ms. Christine Varney
Partner
Hogan and Hartson

Ms. Tova Wang
Vice President of Research
Common Cause

Dr. Michele Waslin
Senior Policy Analyst
Immigration Policy Center

Mr. Dan Weitzner
Technology and Society Policy Director
World Wide Web Consortium

In addition, for comments on biometrics the authors thank:

Mr. Terrance E. Boult
El Pomar Professor of Innovation and Security
University of Colorado at Colorado Springs

Finally, the authors extend their thanks to their colleagues: Rhonda Carter, PJ Crowley, Ed Paisley, and Michael Rugnetta for their important contributions to securing the successful completion of this phase of the Progressive Identity Project.

Endnotes

1 Stephen T. Kent and Lynette I. Millett, eds., *Who Goes There? Authentication through the Lens of Privacy* (Washington, DC: Computer Science and Telecommunications Board, National Research Council, National Academy of Sciences, National Academies Press, 2003), available at http://books.nap.edu/openbook.php?isbn=0309088968.

2 Stephen T. Kent and Lynette I. Millett, eds., *IDs -- Not That Easy: Questions About Nationwide Identity Systems* (Washington, DC: Computer Science and Telecommunications Board, National Research Council, National Academy of Sciences, National Academies Press, 2002), available at http://www7.nationalacademies.org/cstb/pub_nationwideidentity.html.

3 Richard Willing, "Airline ID Requirement Faces Legal Challenge," *USA Today*, October 11, 2004, available at http://www.usatoday.com/news/nation/2004-10-10-privacy_x.htm. In 2006, the Department of Homeland Security clarified that showing ID is not required to fly on an airplane, but passengers who don't show ID will be subject to secondary screening. *Gilmore v. Gonzales*, 435 F.2d 1125 (9th Cir. 2006).

4 http://www.epatric.com/funstuff/dog/

5 In April of 2006, 62 percent of respondents to a national poll strongly favored the showing of photo identification before voting, 19 percent somewhat favored, 12 percent were neutral, 3 percent somewhat opposed, and only 4 percent strongly opposed. Peter Hart and Bill McInturff, NBC News/Wall Street Journal Survey, Study # 6062, at 13 (2006), available at http://online.wsj.com/public/resources/documents/poll20060426.pdf.

6 Sophia Cope, "The Impact of Implementation: A Review of the REAL ID Act and the Western Hemisphere Travel Initiative," Testimony to the Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, April 29, 2008, available at http://www.cdt.org/testimony/20080429scope-written.pdf.

7 For instance, the Internal Revenue Service reported an increase of 644 percent in identity theft cases from 2004 to 2007. Many of the cases involved misuse of another person's Social Security number to get a refund. BNA Privacy Law Watch, "IRS Plans to Open Specialized Unit for Handling Identity Theft Cases," May 9, 2008.

8 Federal Trade Commission, "2006 Identity Theft Survey Report" (2007), available at http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

9 In 2007, identity theft complaints totaled 32 percent of all consumer complaints. Federal Trade Commission, "Consumer Fraud and Identity Theft Complaint Data, January - December 2007" (2008), available at http://www.ftc.gov/opa/2008/02/fraud.pdf.

10 Harris Interactive, "Identity Theft: New Survey & Trend Report" (2003), available at http://www.bbbonline.org/IDTheft/IDTheftSrvyAug03.pdf.

11 Theft of Rep. Anna Eshoo's (D-CA) Social Security number contributed to passage of financial privacy protections. Chris Jay Hoofnagle and Emily Honig, "Victoria's Secret and Financial Privacy" (2005), available at http://epic.org/privacy/glba/victoriassecret.html.

12 Michael E. Jones, "Data Breaches: Recent Developments in the Public and Private Sectors," *I/S: A Journal of Law and Policy for the Information Society* 555 (2007-2008).

13 Privacy Rights Clearinghouse, "A Chronology of Data Breaches," available at http://www.privacyrights.org/ar/ChronDataBreaches.htm.

14 See World Privacy Forum, "The Medical Identity Theft Information Page," available at http://www.worldprivacyforum.org/medicalidentitytheft.html.

15 Thomas Claburn, "Congressional Report Slams TSA for Security Breach," Information Week, January 11, 2008, available at http://www.informationweek.com/news/security/showArticle.jhtml?articleID=205602931.

16 One report estimates that 22 million voting-age citizens lack a driver's license. Brennan Center for Justice at NYU School of Law and Spencer Overton, "Response to the Report of the 2005 Commission on Federal Election Reform 24 n.9" (2005); Task Force on the Federal Election System, "To Assure Pride and Confidence in the Electoral Process: Task Force Reports to Accompany the Report of the National Commission on Election Reform" (2001), Ch. 6, available at http://www.millercenter.virginia.edu/programs/natl_commissions/commission_final_ report/task_force&uscore;report/task_force_complete.pdf.

17 According to the Federal Highway Administration, 13.2 percent of U.S. residents 16 years and older lacked a driver's license. Commission on Federal Election Reform, "Building Confidence in U.S. Elections 73 n. 22" (2005), available at http://www.american.edu/ia/cfer/report/full_report.pdf; Federal Highway Administration, U.S. Dept. of Transportation, "Licensed Drivers by Sex and Ratio to Population—2003" (2004), available at http://www.fhwa.dot.gov/policy/ohim/hs03/pdf/dl1c.pdf.

18 Diana M. Zuckerman, "Blind Adults in America: Their Lives and Challenges," (Washington, DC: National Center for Policy Research for Women & Families, 2004), available at http://www.center4research.org/blind0204.html.

19 According to a recent study, 19 percent of legally blind persons live in poverty. Ibid.

20 Spencer Overton, "Voter ID Supporters Lack Hard Evidence," available at http://docs.law.gwu.edu/facweb/soverton/ajc_april8_2005.pdf.

21 One study reports that 91 percent of the state's elderly without a driver's license are white. John Pawasarat, "The Driver License Status of the Voting Age Population in Wisconsin," Employment and Training Institute, University of Wisconsin-Milwaukee (2005), available at http://www.brennancenter.org/page/-/d/download_file_50902.pdf.

22 Simson L. Garfinkel, "Nobody Fucks with the DMV," Wired, Feb. 1994, available at http://www.wired.com/wired/archive/2.02/dmv.html.

23 Ibid.

24 For instance, the rate of duplicate individual licenses in 2007 was 24.2 percent for Alaska (36,784 out of 151, 502). Stacy Oates, interview with Alaska Department of Motor Vehicles, Washington, D.C., May 19, 2008. For Florida, duplicates for the 2005-06 fiscal year were 19.4 percent (1,045,296 out of 5,380,905). http://www.flhsmv.gov/html/FactsFiguresFY2006/PerStaDDL.htm. For Idaho, duplicates in 2006 were 19.8 percent (46,319 out of 187,345), http://www.itd.idaho.gov/econ/DriversLicense/DLISS06.xls. For Wisconsin, duplicates for 2006 were 25.6 percent (322,201 out of 1,258,278), http://www.dot.state.wi.us/drivers/docs/drlicissue.pdf.

25 Brennan Center for Justice, "Citizens Without Proof: A Survey of Americans' Possession of Documentary Proof of Citizenship and Photo Identification" (2006), available at http://www.brennancenter.org/page/-/d/download_file_39242.pdf.

26 Pawasarat, "The Driver License Status of the Voting Age Population in Wisconsin," p. 2.

27 Matt A. Barreto, Stephen A. Nuno, and Gabriel R. Sanchez, "The Disproportionate Impact of Indiana Voter ID Requirements on the Electorate" Working Paper (Washington Institute for the Study of Ethnicity and Race, 2007), available at http://depts.washington.edu/uwiser/documents/Indiana_voter.pdf.

28 Anne Broache, "Religious minorities face REAL ID crackdown," CNet, Feb. 6, 2008, available at http://www.news.com/Religious-minorities-face-Real-ID-crackdown/2009-1028_3-6229258.html.

29 General Accountability Office, *Medicaid: States Reported That Citizenship Documentation Requirement Resulted in Enrollment Declines for Eligible Citizens and Posed Administrative Burdens*, (June, 2007); See also, Robert Pear, "Citizens Who Lack Papers Lose Medicaid," *New York Times*, March 12, 2007.

30 Ibid. p. 5.

31 Brennan Center for Justice, "Citizens Without Proof: A Survey of Americans' Possession of Documentary Proof of Citizenship and Photo Identification"

32 U.S. Department of State, "Passport Fees," available at http://www.travel.state.gov/passport/get/fees/fees_837.html.

33 Ibid.

34 "Preventing Identity Theft by Terrorists: Joint Hearing on SSNs and Identity Theft," Hearings before the Subcommittee on Oversight and Investigations of the House Committee on Financial Services, and the Subcommittee on Social Security of the House Committee on Ways and Means, 107th Cong. 1 Sess. (statement of Marc Rotenberg, Executive Director, Electronic Privacy Information Center), available at http://financialservices.house.gov/media/pdf/110801mr.pdf.

35 Elise Chidley, "Data Integrity and the Enterprise MPI," *For the Record*, June 29, 1999, available at http://www.sice.umkc.edu/~leeyu/Mahi/medical-data4.pdf.

36 "Retired fireman's identity mired in 40-year-old-fudge," *Chicago Sun-Times*, March 21, 2006, available at http://realnightmare.org/images/File/IL%20sun%20times%20retired%20fireman.pdf.

37 Brennan Center, "Making the List," available at http://www.brennancenter.org/makingthelist.html.

38 National Immigration Law Center, "Basic Pilot/E-Verify: Not a Magic Bullet," (January 2008), available at http://www.nilc.org/immsemplymnt/ircaempverif/e-verify_nomagicbullet_2008-01-04.pdf.

39 Ibid.

40 Findings of the Basic Pilot Program Evaluation, (Temple University Institute for Survey Research and Westat, June 2002), available at www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=9cc5d0676988d010VgnVCM10000048f3d6a1RCRD&vgnextchannel=2c039c7755cb9010VgnVCM10000045f3d6a1RCRD; Findings of the Web-Based Basic Pilot Evaluation, (Westat, September 2007), available at www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=89abf90517e15110VgnVCM1000004718190aRCRD&vgnextchannel=a16988e60a405110VgnVCM1000004718190aRCRD; Congressional Response Report: Accuracy of the Social Security Administration's Numident File, (Office of the Inspector General, Social Security Administration, December 2006), available at www.socialsecurity.gov/oig/ADOBEPDF/audittxt/A-08-06-26100.htm; Congressional Response Repot: Employer Feedback on the Social Security Administration's Verification Programs, (Office of the Inspector General, Social Security Administration, Dec. 2006), www.ssa.gov/oig/ADOBEPDF/A-03-06-26106.pdf; Congressional Response Report: Monitoring the Use of Employee Verification Programs (Office of the Inspector General, Social Security Administration, September 2006), available at www.ssa.gov/oig/ADOBEPDF/A-03-06-36122.pdf.

41 "About the Issue: Real Stories," available at http://www.realnightmare.org/about/4/.

42 Ibid., quoting "Mismatched Records May Cost Hoosiers Their Licenses," *The Indianapolis Star*, November 2, 2007.

43 Luiz Casanova, Lieutennant, New Haven Police Department (NHPD), Affidavit, "Municipal ID,", January, 2008, available at http://www.americanprogress.org/issues/2008/06/pdf/casanova_affidavit.pdf; Francisco Ortiz, Chief of Police, New Haven Police Department (NHPD), Affidavit, "Municipal ID,", January, 2008, available at http://www.americanprogress.org/issues/2008/06/pdf/ortiz_affidavit.pdf.

44 One example is the payment technology described in: Stefan Brands, *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy,* (Cambridge, MA: MIT Press 2000), available at http://www.credentica.com/the_mit_pressbook.html.

45 For a due diligence checklist for new information sharing programs, including identification programs, see: Peter P. Swire, "Privacy and Information Sharing in the War Against Terrorism," 51 Villanova L. Rev. 260 (2006), available at http://ssrn.com/abstract=899626.

46 The term "shared secret" is used here in a broader way than it is technically used in the field of cryptography. In cryptography, a "shared secret" is most commonly used to refer to a symmetrical encryption key. In this report, the term refers to something, such as a mother's maiden name, that is supposed to be secret but may in fact be known more widely.

47 http://genealogy.about.com/od/surnames/tp/maiden_names.htm.

48 One report concludes that holding fingerprints in databases is generally insecure and should be used as rarely as possible. Ann Cavoukian and Alex Stolanov, "Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy," (March 2007), available at http://www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf.

49 A 2004 report by the National Institute for Standards and Technology found that the accuracy rate for fingerprint identification drops as the age of the person increases, especially for those more than 50 years old. http://epic.org/privacy/biometrics/.

50 T.E. Boult, W.J. Scheirer, and R. Woodworth, "Revocable Fingerprint Biotokens: Accuracy and Security Analysis," (IEEE Conference on Computer Vision and Pattern Recognition, 2007).

51 http://www.schneier.com/crypto-gram-0205.html#5.

52 http://www.privacyrights.org/ar/ChronDataBreaches.htm. For a survey of the high costs to businesses of data breaches, see: Ponemon Institute, "Ponemon Study Shows Data Breach Costs Continue to Rise," November 28, 2007, available at http://www.ponemon.org/press/PR_Ponemon_2007-COB_071126_F.pdf.

53 http://www.cdt.org/privacy/authentication/030513interim.pdf.

54 Ibid. The Center for Democracy & Technology, which led the working group, has released a draft for comment to update those principles. CDT, "Privacy Principles for Identity in the Digital Age, Draft for Comment - Version 1.4" (December 2007), available at http://www.cdt.org/security/identity/20080108idprinciples.pdf.

55 National Academy of Sciences, National Research Council, "Who Goes There? Authentication Through the Lens of Privacy" (2003), p. 188.

56 There are numerous initiatives underway for these sorts of authentication for online activities, including OpenID, CardSpace, and the Liberty Alliance. Especially promising technologies for authentication are based on the work of cryptographers Stefan Brands and David Chaum. The Transportation Safety Administration has recently taken a promising step in the direction of using device-based authentication. It is now testing using barcodes in a Blackberry or similar device as a replacement for paper boarding passes. TSA reports that the device-based approach leads to higher security as well as avoiding the cost of printing the paper passes. Susan Stellin, "Paper is Out, Cellphones are In," *The New York Times,* March 18, 2008, C6.

57 The systems would have to be secure in the event that a cellphone was stolen or lost. A good defense against theft of the passwords is for the device to require a PIN in order to access the passwords. To prevent against loss of the passwords will take better backup measures than many individuals use today.

58 Ga. Code Ann. §21-2-417 (amended 2005); Ind. Code Ann. §3-11-8-25.1 (amended 2003); Mo. Ann. Stat. §115.427 (amended 2002).

59 Tova Andrea Wang, now of Common Cause, has collected sources at: http://www.tcf.org/list.asp?type=IN&pubid=%7B647BD6E5-371F-434E-B9D5-5B09E3FFC363%7D.

60 Spencer Overton, "Voter Identification," 105 Mich. L. Rev. 631 (2006), available at http://ssrn.com/abstract=908371.

61 Ibid., p. 635.

62 Tova Andrea Wang, "Where's the Voter Fraud?" (December 4, 2006), available at http://www.tcf.org/list.asp?type=NC&pubid=1452.

63 Mark Follman, Alex Koppelman, and Jonathan Vanian, "How U.S. attorneys were used to spread voter-fraud fears," *Salon*, March 21, 2007, available at http://www.salon.com/news/feature/2007/03/21/us_attorneys/. Josh Marshall, TalkingPointsMemo, April 12, 2007, available at http://www.talkingpointsmemo.com/archives/013581.php. Lorraine C. Minnite, "The Politics of Voter Fraud," (March 2007), available at http://projectvote.org/fileadmin/ProjectVote/Publications/Politics_of_Voter_Fraud_Final.pdf.

64 Justin Levitt, "Analysis of Alleged Fraud in Briefs Supporting *Crawford* Respondents," (Brennan Center for Justice), December 31, 2007, available at http://truthaboutfraud.org/pdf/CrawfordAllegations.pdf.

65 Ibid.

66 Borders v. King County, No. 05-2-00027-3 (Wash. Super. Ct. Chelan County June 24, 2005). Similarly, a survey of each of Ohio's 88 county Boards of Elections found only four instances of ineligible persons attempting to vote out of a total of 9,078,728 votes cast in the state's 2002 and 2004 general elections. This is a fraud rate of 0.000044%. Coalition on Homelessness and Housing in Ohio & League of Women Voters of Ohio, "Let the People Vote: A Joint Report on Election Reform Activities in Ohio" (2005), available at http://www.cohhio.org/alerts/Election%20Reform%R eport.pdf.

67 Overton, p. 635.

68 http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_twic.pdf.

69 P.J. Crowley, "Marking Our Ports a Priority," (Center for American Progress, July 1, 2004), available at http://www.americanprogress.org/issues/2004/07/b106593.html.

70 http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_twic.pdf.

71 Ibid.

72 The other inclusion concern is that the security risk assessment may sweep too broadly, such as by disqualifying applicants who have long-ago drug or firearms convictions. In light of the high rate of incarceration in the United States, and the importance of re-integrating ex-offenders into society, identification systems should not become a tool for preventing rehabilitation for those who have served their terms.

73 http://www.teamster.org/divisions/rail/pdfs/070307_tolmantestimony.pdf.

Center for American Progress

ABOUT THE CENTER FOR AMERICAN PROGRESS

The Center for American Progress is a nonpartisan research and educational institute dedicated to promoting a strong, just and free America that ensures opportunity for all. We believe that Americans are bound together by a common commitment to these values and we aspire to ensure that our national policies reflect these values. We work to find progressive and pragmatic solutions to significant domestic and international problems and develop policy proposals that foster a government that is "of the people, by the people, and for the people."

Center for American Progress
1333 H Street, NW, 10th Floor
Washington, DC 20005
Tel: 202.682.1611 • Fax: 202.682.1867
www.americanprogress.org