

National ID Briefing

Introduction

The introduction of the Real ID act in 2002 threw the public and the media into a frenzy as they discussed the implications of a national identification system for the United States. Would such a system prevent terrorism? Would it lead to a gross invasion of privacy? Would it allow the government to collect details of people's daily lives? Or would it just be one more card to lose and one more number to remember in an increasingly indexed and identified society? Would it stem the tide of illegal immigrants or would forgery make it easier for illegal immigrants to appear legitimate? Such a novel concept, everyone cried, demands closer attention and study. We are now in the fifth year of this controversy, and there appears to be no end in sight.

Unfortunately, the debate about national identification schemes faces a major roadblock. There is little consensus on what a national identification system is—the vital elements, the optional add-ons, etc. One paper, published in support of Real ID, alluded to “a national ID, which by definition, must be presented to police on demand at any time....” One must then ask why a national ID system must have such a property. In the absence of a widely-accepted definition for national ID, people getting involved in the debate invent their own assumptions and argue from them without articulating them. In designing a national ID system, many different building blocks could be included, each carrying its own costs and benefits. We hope to define some of these key building blocks and suggest how a national ID system could be designed without reliance on preconceived notions.

Basic Technical Building Blocks

Tamper-Resistant identification—A physical form of identification which is difficult to copy (create a duplicate of an already-existing ID), difficult to forge (create an ID with a new combination of information), resistant to fraudulent use (using someone else's ID, or using an expired or otherwise invalid ID), and difficult to obtain. Each of these aspects has its own impediments to achievement, and whether perfect security in any of these senses can be achieved is certainly debatable. This identification card (we will assume it to be a card, but there are certainly other forms possible) will convey some minimal set of information, including name, address, and birth date.

- **Difficult to copy:** As seen in the history of currency, the elements that make a document hard to copy change over time. They range from the use of rare materials to microprinting and holograms.
- **Difficult to forge:** Something that is difficult to copy will almost assuredly be difficult to forge. In addition, stricter resistance to forgery can be had by applying a transformation to data displayed on the card (i.e. text that is rotated slightly, or pictures which are pixellated according to a specific algorithm such that they are recognizable under scrutiny). Further security can be had by encrypting the data stored on the card.

- Difficult to use fraudulently: the addition of pictures to many standard forms of ID is one move in this direction. Additional approaches might include the use of biometric identifiers such as fingerprint, retinal scan, or DNA coding
- Difficult to obtain: Today, the Department of Motor Vehicles is engaged in such a fight against their reputation of poor customer service that they often feel obliged to speed through the process of issuing drivers' licenses without thoroughly checking identity documents that applicants must present. This makes drivers' licenses easier to obtain practically than they are theoretically. A secure system would have stringent requirements for proving one's identity before issuing, would enforce document verification, and have a way of dealing with lost cards that was comparable in strictness.

Standardized, Machine-Readable Data—Current implementations of this form include cards with swipe strips for magnetic readers, and cards with some form of RFID (radio-frequency identification) technologies built into them. Some current forms of identification (most notably, drivers' licenses) have no consistent data format used across the nation. Passports, issued by the federal government, have a standard form, but only have only recently been made machine readable.

Unique Identifier—A number or string which is assigned to one person, and one person only. May or may not convey any information about the individual in the way it is formulated (the US Social Security Number, not a unique identifier, provides information about where a person was likely born). Must have a wide addressing space to provide for current and future users.

Database—Additional information about individuals, linked to their national identifier, and available to authorized users. This may be a closed database, containing limited information from federal records, or an open database in which trusted parties such as health-care professionals can add information.

Basic Policy Building Blocks

As important as the technological decisions about the capabilities of a national identification system are decisions about the legitimate use of the system. We focus on legislation of appropriate third party use.

Not utilized by the private sector—Legislation prevents all use of information from the national identifier (or protects it, as is currently the case with SSNs), including any potential unique identifiers.

Private sector use for identification/authentication only—Third parties would be able to ask for a person's identifier and use the information contained within, but they would not be able to store any of the information. Thus, a business could not collect customer profiles, or create their own database of information keyed on people's National ID numbers. Authentication implies ensuring not only that a person is who she says she is, but also ensuring that she is authorized for whatever action she is attempting, whether it is entering a bar or renting an R-rated movie, or purchasing a gun or toxic substance.

No legislation on private sector use—The private sector is able to use data from the National ID for their own purposes, including storing that information and creating additional databases, which may or may not be linked back to a national database.

Proposed National ID schemes in the United States

In 2002, a bill standardizing state driver's license cards and databases known as "The Driver's License Modernization Act" was submitted to Congress. The Electronic Frontier Foundation described the bill as follows: "Though it differs in some interesting particulars, [the Act] is like all other proposals for a national ID system, in that it promises to salve the most pressing problem of the hour. This year, a national ID system will fight terrorism; in calmer times, it promised to make health care affordable, borders secure, illegal immigrants tractable, or deadbeat dads traceable." Many national ID programs proposed in the United States have been promoted with exaggerated benefits and only a cursory examination of the costs.

Social Security—The Social Security Act of 1935 instituted a system to register workers so that they could receive Social Security after retirement. The information collected for the Social Security Administration, including income, was proclaimed private at the outset, however it has been increasingly released to government and other agencies. Other agencies have taken to co-opting the social security number, which functions almost as a national ID number because almost all adults have one, for their own purposes. This practice has been cracked down upon recently with upswings in identity theft making individuals more protective of this number. Social Security numbers provide the best evidence of so called "feature creep," that is, a system being used for other than what it was designed for, including the "Parent Locator Service," in essence a way to track down deadbeat dads, established by Congress in 1975. Several times in its history, legislators have proposed making Social Security a real, rather than a de facto, national ID scheme. However, such plans have failed time and again, due to concerns about privacy, and pessimism about benefits.

National worker registration database – In 2005, Congress discussed the idea of implementing a database that would match individuals' social security numbers to their work eligibility status. Employers would be required to consult the database before hiring any employee, and in order to prevent the use of false SSNs, some form of national identification card would be implemented. The program was criticized because it allowed government to interfere in the private contractual agreement between employer and worker, and the program's ability to deter illegal immigration was also called into question. Many illegal immigrants are hired by employers who are fully aware that their new employees are not legally eligible to work, yet the employers still hire knowing they can pay sub-minimum wages. It is unlikely that such employers would be deterred by a national worker registration database.

Health security card – In 1993, the Clinton administration endorsed the idea of creating a national health insurance program for all Americans. An individual would be guaranteed coverage regardless of employer or age so long as he carried a "Health Security card."

While the Clinton administration did not clearly articulate what data the card would contain, opponents feared it could contain sensitive health information and threaten the privacy of medical data. Just as SSNs started as an identifier for benefits eligibility and became a near-national identifier, privacy activists feared Health Security cards would become an even more pervasive means of identification.

Real ID – The Real ID Act of 2005, heralded as the latest incarnation of National ID, requires all state driver’s licenses to meet minimum federal standards by 2010. Before issuing a license, state DMVs first must verify address, DOB, SSN, and legal immigration / residence status of the applicant. The license itself must include tamper-resistant features (possibly biometrics) and store data following a “common machine-readable technology” as defined by the department of Homeland Security. DMVs would be required to share individual driving records with DMVs of other states, but the act does not mandate a national database of information on drivers. A state still has the option to issue driver’s licenses that do not meet federal standards, but such licenses will not be valid at any junctures where a federally-approved ID is required. These junctures include: entrance into airports and courthouses, application for receipt of federal benefits, verification of eligibility of employment, and verification of identity by a bank. The Act has been criticized for the heavy burden placed on DMVs, regulations that make it essentially impossible to not carry a federally-approved ID, and Real ID’s potential to evolve into an invasive government tracking system.

National ID in the UK

In 2006, legislation was passed in Great Britain to allow the issuing of a national ID. Each ID is linked to a person’s National Identity Register, a database with up to 50 pieces of information about each individual. The introduction of the system has incurred much opposition, as Britain would be only the fifth common law country to adopt national IDs in peacetime. Government officials have argued about its efficacy. Other principal concerns are cost, the effect on ethnic minorities (particularly gypsies and other migrant groups who may not be able to inform the government every time they relocate), the wide availability of information, feature creep, vulnerable individuals (such as an abused spouse), and the unproven nature of the technology.

National ID in France

France offers non-compulsory identity cards that contain one’s photo, name, and address. When one applies for the ID card, one’s fingerprints are taken and stored in a secure database that can only be accessed by a judge. The information contained on the card is also stored in a database, but access to this database is strictly controlled and laws prevent the data being linked to other databases. While the card is not compulsory, French police may require an individual to present the ID card and arrest him if he does not possess the card. The French government has plans to implement a “secure electronic national identity card” this year, which would contain biometric data on a chip in the card and in a national database. The card would also contain a digital signature that could be used for signing official documents such as tax documents and private correspondences. While a poll in 2005 suggested that almost 75% of French citizens supported the new cards, a number of French bodies petitioned against the cards. These opponents contended that

the new cards would have limited effectiveness in combating fraud and terrorism, would threaten the privacy of individual information with the central database, and would also threaten the social pact between the citizen and the state.

National ID in China

Since 1985, China has issued ID cards that contain information on one's nationality, birth date, and an 18-digit identification number. In recent years, China has extended the ID cards to include an RFID chip containing personal information that is also recorded in a national database. The government plans to issue RFID scanners to all its police, asserting that the new cards will help deter crime and prevent identity theft. However, opponents are suspicious that the new cards will allow the government to more easily track dissidents. After pro-democracy protests in 1989, the government displayed photos and ID numbers of student protest leaders on television who were wanted by the government. In 2006, the government considered a law that would require all online bloggers to register their national ID numbers before creating a blog. While the bloggers could write under a pseudonym, the government would have access to a database of pseudonyms and national IDs that would enable them to punish any bloggers who authored "illegal" content.

In the following sections, we highlight major costs and benefits of national ID systems that could come about through certain combinations of building blocks.

Cost: Government tracking its citizens

Needed: National ID card with easy swipe or RFID, unique identifier, private sector free to use National ID numbers for its own purposes

The most widely cited cost of any national ID system in the United States is the government's potential to use such a system for tracking the movements and activities of its citizens. At first glance, the skeptic may reason that this potential does not exist if the national ID system is carefully designed not to include tracking capabilities – the government simply does not build a network of ubiquitous ID scanners. The first problem with this "design" argument is that identification schemes have a history of ballooning to uses beyond their original purpose: a decade after the rollout of national ID cards, lawmakers facing new terrorist threats might be tempted to build a network of scanners, knowing that every person already carries an ID card with standardized, machine-readable data. Take the example of social security numbers. These were first issued as identifiers to determine eligibility for social security benefits, but in the 1960s SSNs were used by the Civil Service Commission to identify federal employees and the IRS began requiring SSNs on tax returns. SSNs were subsequently used on driver's licenses, motor vehicle registrations, and private businesses, educational institutions, and medical facilities began using SSNs as an index into their personal files. Simply because a national ID system is designed not to be a tracking system does not safeguard against future adaptations to that purpose.

Yet one might argue that it would be too expensive for the government to rollout a nationwide network of scanners. If the government employed RFID technology, there

would be massive costs in manufacturing large numbers of scanners and in storing huge databases of people's locations and activities. Furthermore, it would seem difficult for the government to make a firm case for a nationwide network of scanners. Would knowing a person's favorite shops or movies identify him as a terrorist? Is such detailed data really needed to determine whether a new school or highway should be built? Finally, one might argue that a government-built scanner network would almost certainly run afoul of the privacy expectations of most American citizens well into the future. Is the threat of government being able to track its citizens with national ID just another hype blown out of proportion?

The most serious threat of government tracking comes not from the government itself but from the private sector. Consider how the government today purchases data from aggregators like ChoicePoint, allowing it to accumulate information that by law it cannot obtain on its own. If the government issued national ID cards with unique identifiers stored on RFID chips, then private businesses would be tempted to use the cards for their own data tracking purposes. For instance, Walmart might install RFID readers at each of its checkout counters, scan ID cards as shoppers passed through, and label each item ordered with a person's ID number in its databases. The company would then be able to obtain more precise statistics on customer flow and offer targeted advertising, yet such information would not only be useful to Walmart but to the government as well. Walmart might resell its data to aggregators like ChoicePoint, and if ChoicePoint receives data from enough businesses and correlates the data by ID number, then it could neatly plot out a person's daily whereabouts. The government could then purchase this ready-made tracking information in a neat package, avoiding the high costs of deploying its own network of scanners or the opposition of privacy activists. This threat does not seem so far-fetched given that the government today purchases data on individuals from ChoicePoint.

Cost: Overconfidence in the system

Needed: Tamper-resistant ID with biometrics/encryption

A less hyped cost of a national ID system concerns public belief in the reliability of the system. If national ID cards are designed to be tamper resistant, including elements such as biometrics and encryption, then people may come to believe that ID cards cannot be forged and that ID-linked data must be accurate. Yet the Electronic Frontier Foundation notes that "a cruel paradox of identity card systems is that the more secure a card is, the greater its value, and the greater the incentive and reward for breaking the card." Criminals (perhaps with insider help from the ID issuing organization) may discover a means to forge an ID card even with encryption and biometric data. The bearer of the stolen identity would face an immense uphill battle to reclaim his innocence, perhaps much steeper than that faced by identity theft victims today. Tamper-resistant IDs would likely cause the number of cases of identity theft to decrease, but general overconfidence in the reliability of the ID system could make each individual case of identity theft more damaging.

Consider the case of Terry Dean Rogan. In the early 80s, Rogan lost his wallet and driver's license in Detroit, and nearly a year later, a murderer used these documents while he committed crimes and evaded capture. One evening, police came to Rogan's home in Los Angeles to answer a routine noise complaint, but when they checked his ID in the FBI's criminal database, Rogan came up as a wanted murderer. He was arrested and was about to face trial when the police discovered that his fingerprints did not match those left by the murderer at the scene of the crime. Unfortunately for Rogan, the LA police department failed to notify the FBI that Rogan was cleared of the charges, causing Terry to be arrested four more times over the next 14 months after routine traffic stops.

This case illustrates two dangers to overestimating the reliability of ID. First, if there is an error in the system (i.e. the LAPD fails to notify the FBI), then an individual may incur significant costs while trying to resolve it, costs that increase with the perceived reliability of the system (LAPD arrests immediately based on data from the FBI crime database). Second, Terry was only saved from defamation and possibly jail by his fingerprints. If a talented criminal had managed to even forge Terry's fingerprints, what jury would think twice about convicting him?

An instance where biometrics have been used to convict a potentially innocent person follows. A brutal string of murders in Michigan in the 1970s went unsolved for decades, until police investigators decided to reopen the case in recent years, knowing they could use DNA evidence from the victim's body to search across a database of DNA samples. The investigators were overjoyed when they found a match, a father who no longer lived in Michigan but had lived there in the 1970s. While he had no previous criminal record and there was no other evidence to connect him to the crime, a jury convicted him of murder and he remains in jail today. While the case against the defendant may seem convincing, the prosecution failed to explain one important piece of evidence. Some DNA left on the victim's body matched the defendant's, but other DNA was matched up to a man who would have been four years old and lived in California at the time of the murder. It seems completely incomprehensible that the boy could have been present at the murder scene, calling into question the DNA collection and analysis process. Perhaps the DNA matching algorithms identify a match too easily, perhaps the samples or lab equipment were contaminated, or perhaps an enemy of the defendant worked in the DNA lab. Yet all these questions were not enough to create "reasonable doubt" in the minds of the jury. If smart criminals can forge biometrics or criminal investigators simply make mistakes, tamper-resistant ID systems could create huge costs for unfortunate victims of mistaken or stolen identity.

Benefit: Reduction of Identity Theft

Needed: Tamper-Resistant Identification, private sector use for identification / authentication

The Federal Trade Commission estimates that more than 9 million individuals have their identities stolen each year in the United States. Research indicates that this is a growing trend, correlated with the de-personalization of many business transactions, including the rise of electronic commerce. After an identity thief has co-opted someone's personal

information for his own use, whether it be opening a credit card, or renting a car, it can take thousands of dollars in legal fees to undo the damage of a criminal's spending spree.

A national ID, in its ideal form, would counteract the impersonal nature of financial transactions, allowing a vendor to know that the purchaser is who he claims even if they have not lived in the same town together for twenty years, or have not seen each other once a month at the local bar. It would link a physical human being with a set of data irrevocably.

This issue is closely tied with the cost of overconfidence. An "irrevocable link" is positive because it creates one standardized and secure method of verifying someone's identity, but if that security is breached, the cost of "irrevocability" is thrown into sharp relief. As such, the net benefit of national ID legislation has been questioned with respect to identity theft.

Benefit: Better linked threat protection: Gun control and voter fraud

Needed: Tamper-Resistant Identification, national identifier and database, private sector use for identification / authentication

A novel and ill-defined phrase, "threat protection" has two meanings in our analysis. First, a national identification system could protect the government, health care providers, and others from the fraud that plagues their business transactions. Second, it could protect individuals by keeping controlled substances restricted from those who are likely to use them in a dangerous manner.

These problems all stem from similar difficulties. They require a certain set of credentials: identity, background checks, health insurance, etc. Records exist for each of these credentials (or lack thereof, in the case of death certificates and mental health records), but it is difficult to make sure all of the credentials align because different records are owned and kept by different parties. These may all be accessible, but finding them requires inquiring at every possible record-holder in order to establish the necessary collection of relevant information. Creating a better way to link information about a person from the various record-keeping entities would alleviate some of the difficulties faced today.

Perhaps the most pressing recent example of a situation where increased information might have led to a better outcome is the case of the Virginia Tech shooter, Seung-Hui Cho, who on April 16, 2007, shot and killed 32 of his classmates and teachers at Virginia Tech. Cho, who had been involuntarily admitted to a mental health treatment facility, was cleared to purchase a gun, though federal law prohibits "anyone who has been 'adjudicated as a mental defective,' as well as those who have been involuntarily committed to a mental health facility" from purchasing a gun. Despite this legislation, only seventeen states report such mental health records to the office which does the

background checks required for gun purchase. This is done for privacy reasons, but it also undermines the usefulness of these records and the legislation.

Voter fraud (of the less sophisticated variety) also suffers from a lack of connected records. First, voter registration is a process that can be circumvented with a little creativity. Examples abound of third parties registering voters and sending them the cards with information on “the smart vote.” Second, those who were eligible to vote, but have moved or died, are also often found to be voting in their old location. Every month, the state is supposed to send lists of the people who have died to those who supervise the voting process. These lists are typically only sent out once every few months, and between updates, thousands of deceased voters may be given absentee ballots. A national database would be needed to keep this data available at voting stations to deter voter fraud.

Conclusion

We find that the benefits of a national identification system are not as spectacular as many proponents have claimed them to be. While some have proclaimed that a national ID systems could deter terrorism or illegal immigration, we do not find these stories plausible. Some modest benefits like deterrence of identity theft can be had by incurring some modest costs, like overconfidence. Yet can one even call such a system national ID? If one wants to secure more benefits, such as better control of dangerous substances, then one approaches closer to the threat of government tracking by creating a national identifier and associated database. We summarize our basic building blocks and their associated costs and benefits in the chart below. Even if we have missed major costs/benefits in our discussion, we believe our method for analysis (arguing from basic components) presents a better alternative to current debates that are hindered by preconceived notions of national ID.

	<i>Technical</i>				<i>Policy</i>		
	Tamper-resistant ID	Machine readable data	Unique ID	National DB	No Private Sector	Use for ID	No restrictions
Government Tracking		✓	✓				✓
Overconfidence	✓						
Reduce ID theft	✓					✓	
Better linked threat protection	✓		✓	✓		✓	

References

Abernathy, William and Tien, Lee. "National Identification Systems." Electronic Frontier Foundation.

<http://www.eff.org/Privacy/Surveillance/nationalidsystem.html>

McCullagh, Declan. "National ID Cards on the Way?" CNET, Feb 2005.

http://news.com.com/National+ID+cards+on+the+way/2100-1028_3-5573414.html?tag=st.num

Mill, John and Moore, Stephen. "A National ID System: Big Brother's Solution to Illegal Immigration" Cato Institute. September, 1995

<http://www.cato.org/pubs/pas/pa237.html>

"The Real ID Act of 2005". Electronic Privacy Information Center.

http://www.epic.org/privacy/id_cards/

"Real ID, Unrealistic Law" Boston Globe Editorial, Mar 2007.

http://www.boston.com/news/globe/editorial_opinion/editorials/articles/2007/03/20/real_id_unrealistic_law/

"China to issue 1.3 billion RFID identification cards." InfoWorld. March 2006.

http://www.infoworld.com/article/06/03/09/76259_HNchinarfidcards_1.html

"China readies super ID card, a worry to some" The New York Times. August 2003

<http://query.nytimes.com/gst/fullpage.html?res=9E02EEDB1030F93AA2575BC0A9659C8B63&sec=&spon=&pagewanted=2>

Eaton, Joseph. The Privacy Card. Rowman & Littlefield Publishers, 2003.

Etzioni, Amitai. How Patriotic is the Patriot Act? Routledge Publishers, 2004.

Harper, Jim. Identity Crisis: How Identification is Overused and Misunderstood. Cato Institute, 2006.

Privacy Act of 1974, Public Law No. 93-579, 88 Stat. 1897 (Dec. 31, 1974).

Rule, James B. and Douglas McAdam, Linda Stearns, David Uglow. "Documentary Identification and Mass Surveillance in the United States." *Social Problems*, Vol. 31, No. 2. (Dec., 1983), pp. 222-234.