National Identification Systems

A Solution in Search of a Problem.

The EFF views impending moves towards a National ID system with alarm. Public officials, in their zeal to appear to be doing something about terrorism post 9-11, are sending us on a perilous course into a future in which every movement and transaction is subject to monitoring and surveillance. We present here our position on the issue, and online resources designed to help the reader to gain a greater acquaintance with national ID schemes, the latest of which is on the congressional agenda as H.R. 4633 (also known as the Davis-Moran Bill or the Driver's License Modernization Act of 2002). The EFF is a proud member of the National ID Coalition, a broad-based coalition of human rights advocacy organizations from both the left and the right, dedicated to stopping the national ID system.

We Oppose a National ID System

Since September 11th, the nation has struggled to come up with new ideas to prevent such a catastrophe from ever recurring. Disturbingly, many old and repeatedly rejected ideas have reentered the national discourse as well. Among them is the proposed introduction of a national identification card system. EFF opposes any such scheme:

- because no compelling case has been presented for its utility or effectiveness as a crime-fighting tool,
- because of its inevitable costs (in dollars, privacy, and liberty), and
- because of its high potential for abuse, by entities in both the public and private sectors.

Pending Legislation

The most recent incarnation of a national ID system is known alternatively as HR 4633, the Davis-Moran Bill (after its sponsors, Republican Tom Davis and Democrat Jim Moran, both from Virginia) or "The Driver's License Modernization Act of 2002." While the proposed legislation has gained currency due to public concerns over terrorism, it is merely proffering old wares in a new wrapper. In proposing to create a *de facto* national ID system by standardizing state motor vehicle license cards and databases, Davis-Moran rehashes an approach that has been consistently proposed and rejected by Americans throughout the years. Ironically, were a national ID system in place, nothing about the events of 9-11 would have changed. None of the terrorists used fake identification to perpetrate their crimes.

Though it differs in some interesting particulars, HR 4633 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. As always, however, the case for a national ID system is bolstered by airy claims and little by way of proof of the efficacy of such systems. Even in the realm of theory, it's difficult to see how introducing a national ID, even one equipped, as HR 4633 proposes, with biometric identifiers and "smart" chip technology, would pose more than a nuisance to terrorists, particularly those who have yet to do anything to arouse suspicion. Nevertheless, whether a national ID system is built around a card with or without clever technology built in, it will inevitably lend itself to abuse.

Will a National ID system help fight crime?

Before adopting a policy that bears serious civil rights and privacy implications, it's important to have some assurance that it addresses an actual need, and that once implemented it will work as intended. But identification systems rank low on the list of problems facing law enforcement. Though four of the September 11th hijackers legally obtained Virginia driver's licenses under a now-closed state loophole, it is unclear how a national ID would have changed matters -- only two of the nineteen hijackers were on the FBI's terrorist "watch list," and neither of these two were known to have used fake IDs. In fact, one of these watch-listed terrorists was also listed under his own name in the San Diego phone directory*. With hindsight, the obvious flaw was not the lack of a national ID card, but a lack of attentive police and intelligence work.

Proponents promise that a national ID system would be of assistance in tracking the movements of criminals, but to do so would require ubiquitous checking of national IDs, making the national ID card, in essence, an internal passport. To be effective as a tracking tool, a national ID system would have to subject all of us to ubiquitous checkpoints and/or to random ID checks, with police empowered to detain people based on their failure to produce identification. ID challenges would have to become commonplace, a police power that has historically been anathema to free societies. A system of ID challenge, inevitably, rests on the individual judgments of police to decide who "looks suspicious" enough to challenge for ID, opening a new avenue for racial profiling. Likewise, bureaucrats dispensing public benefits and services would also come to rely on the national ID for verification, adding to the burden on the poor and disenfranchised. These effects alone raise serious doubts about the harmlessness of a national ID system.

How would such a system work?

Any national ID system must be based on four key components:

- an identity verification system
- a database
- a card
- a card verification system.

While the card is the most visible of these components, without the other components working together, the card is not especially useful. Before a card can be issued, there must be some means of assuring that the person receiving the card is who he or she claims to be. Because of this, any ID system is only as good as its ability to verify an identity in the first place. If a terrorist successfully misidentifies himself to the ID system initially, then he is a greater threat than if he had no ID at all, for now he is equipped with a domestic ID that "proves" his false identity. Since the major concern of the present proposal is foreign terrorism, and since foreign nationals' chain of identity begins and ends with their passports, it is hard to see how a national ID system can bring much improvement over existing ID systems in this most crucial first step.

Issuance of the ID is accompanied by the entry of the person's identifying information into a database. But an ID database, no matter how sophisticated, only gives basic information about the person identified: weight, height, hair and eye color, address, etc. It cannot address the focal problem in the hunt for terrorists: figuring out who the terrorists are before they commit a crime. Sorting out the vanishingly small minority of actual terrorists from the millions of ordinary "good guys" in an ID system will never be accomplished by an ID system, but rather through good police and intelligence work. If an ID database is to be used, as some advocates claim, for tracking suspected terrorists, those terrorists would still need to be identified first, and then tracked, as tracking the daily movements of over 270 million people would represent an inconceivably large undertaking.

Proponents of new national ID systems believe that adding technological features to the cards themselves will eliminate problems inherent to such systems, like fraud and forgery. History does not smile on this belief. If a card can be affordably mass-manufactured, it can also be forged. The addition

of "high-tech" features--embedded "smart" chips, biometric interlocking, and linking of card data to databases--all promise to make cards less forgeable, and for a while will succeed. However, 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. Any card or device in the public's hands long enough will be cracked. The more secure the card, the more expensive it will be to roll out, and the more costly will be its eventual failure.

Finally, deriving any value from building enhanced high-tech security measures into a national ID system will require a massive card verification architecture. Putting a microchip on an ID card only improves it if there is a fair chance that a police officer, airport gate worker, or other person who should have cause to inspect the card has a machine capable of reading its advanced features. Unfortunately, federal ID mandates frequently run afoul of funding problems. Notwithstanding the expenditure of over a billion dollars on a program to update the "green card," the Immigration and Naturalization Service's new, tamper-resistant high-tech card has a fatal flaw: few at the INS have been issued the equipment needed to read the card's high-tech features. † Building the card-verification infrastructure to make the cards work adds more to the overall cost of the system. Much of these costs would have to be picked up by police departments at the state and local level.

On a national scale, rolling out such ubiquitous technology represents a massive expense, and yet, if one or more of the card's features is invalidated by forgery, the integrity of the entire system is eroded. Given the ever-accelerating pace of technological innovation, building hundreds of millions of "smart" cards in the expectation that they will stay ahead of forgers is a reckless course, one likely to lock us into a string of costly failures.

Selling the Goods

The easiest method of imposing a national ID system, of course, is not to impose one at all, but rather to modify existing ID systems. Davis-Moran follows this course, leveraging both the widespread acceptance and the pre-built infrastructure of state drivers' license and ID card offices, and authorizing some $300 million in federal grant money to finesse the deal. Though this sum is only a fraction of most estimates of the cost of implementing a national ID, and the states may well be left making up the difference, not everyone in state government is displeased with the federal mandate. The American Association of Motor Vehicle Administrators, an association that represents the interests of motor vehicle administrators in the US and Canada, has been a vocal proponent. Also swept up in the wave of patriotic national ID fervor are CEOs Larry Ellison of Oracle and Scott McNealy of Sun Microsystems, who likewise stand to profit handsomely from the sales of the software, services, and hardware required to create such a massive information architecture.

Under Davis-Moran, drivers' licenses would include an embedded microchip possessing all information printed on the front of the card, plus reference biometric information. Additionally, the Davis-Moran bill calls for the chip to "accept data or software written to the license or card by non-governmental devices if the data transfer is authorized by the holder of the license or card." This feature appears to be a ploy to drive commercial acceptance of the national ID card and to make its use more commonplace and accepted as a ubiquitous means of electronic verification. Widespread and accepted use in commerce would also make the card more useful as a surveillance tool.

But what would constitute a cardholder's authorization to write to the card? A recent New York Times article‡ revealed that Boston area bartenders, while using a magnetic card stripe reader to "verify" their patrons' state driver's licenses are also, without patrons' knowledge or consent, collecting their personal data (including home address, sex, height, weight, and physical appearance) for marketing purposes. Does merely handing a businessman your ID card "authorize" him to sell your home address to junk mailers? And what, given such a tenuous "authorization," and the write-enabled ID card envisioned by Davis-Moran, could a merchant write to your ID card for the next reader-equipped merchant or government authority to read?

Function Creep

This raises one of the great problems of national ID programs. Once implemented, programs take on lives of their own. If a system is implemented that provides a single nationwide unique numeric identifier, that system will become a prime focus for businesses, and shortly afterwards, a target of identity thieves. On its introduction, the Social Security number was intended merely to ensure workers paid into the system, and that when the need arose, they could be paid their benefits. Despite its humble origins, however, the simple, nine-digit SSN has grown to become a shadow national ID, a prerequisite for taxation and the provision of a host of government services, coopted by private database maintainers as the key to massive amounts of personal data.

Clearly, the backers of HR 4633 would like people to use the card system in commerce as well as in their dealings with the government. This would make it very difficult to maintain privacy in personal dealings, and could open up every non-cash transaction to scrutiny by the government and by private data gatherers.

Who Watches the Watchmen?

Even if the system works perfectly, however, interfacing flawlessly designed, uncrackable cards through a secure reader to a database system full only of well-verified, lawful information on citizens, accessible only to properly-authorized civil authorities, one factor can never be engineered away: even a perfectly-built system is corruptible by imperfect individuals. Today, we entrust considerable amounts of personal information to our state and federal governments. Unfortunately, public officials, acting in rash patriotic zeal or for less noble motives, have time and again violated the public's trust. The solemn confidentiality surrounding census data, for instance, was abrogated to round up and imprison Japanese-American citizens during the Second World War, and income tax data has been misused time and again by politicians and IRS investigators alike.

Despite government assurances to the contrary, Lord Acton's maxim, "power corrupts" has time and again proven true. Our best hope is to lead our government not into temptation, and to reject national ID systems before they get started.

* "The Hijackers We Let Escape" (cover story) Newsweek, 6/10/02
† http://www.latimes.com/news/nationworld/nation/la-111901tech.story
‡ "Welcome to the Database Lounge" New York Times: March 21, 2002

Media Coverage/Resources

Check out this page for helpful resources including lots of media coverage and links related to the topic.

Acknowledgements:

This document was written and compiled by William Abernathy and Lee Tien with editorial assistance from Sarah Granger and technical assistance from Johnson Hor.