21. National ID Systems

Policymakers should

- resist identification requirements and data collection, especially biometric data;
- decline to implement the REAL ID Act, defund it, and repeal it;
- abandon the E-Verify background check system; and
- encourage the development and acceptance of private identification systems.

A national identification (ID) card has long been regarded as contrary to the American character, and leading American political figures have opposed it whenever it has been proposed. But the creation of a national ID is becoming more likely with advances in identification technology and the adoption of policies that weave together the constituents of a national ID system or that implement a national ID directly. Avoiding a U.S. national ID requires diligent attention to the privacy costs of identification and tracking policies at all levels of government.

Leading Figures Have Long Opposed a National ID

American politicians across the spectrum have opposed having a national ID, even in the face of promises that such a system would help control illegal immigration. When President Ronald Reagan's attorney general, William French Smith, advocated in a cabinet meeting for support of a national ID card for illegal immigration control, the president reportedly scoffed, "Maybe we should just brand all the babies."

In the same context, Democratic presidential candidate Walter Mondale said, "We've never had citizenship tests in our country before. And I don't think we should have a citizenship card today." Speaker of the House Thomas P. "Tip" O'Neill Jr. (D-MA) said in a 1987 debate over immigra-

tion reform, "Hitler did this to the Jews, you know. He made them wear a dog tag."

A decade before that, conservative eminence Sen. Barry Goldwater (R-AZ) recognized and objected to the surveillance consequences and power shifts caused by national ID systems. In a debate on the Privacy Act of 1974, he said:

> Once the social security number is set as a universal identifier, each person would leave a trail of personal data behind him for all his life which could be immediately reassembled to confront him. Once we can be identified to the administration in government or in business by an exclusive number, we can be pinpointed wherever we are, we can be more easily manipulated, we can be more easily conditioned, and we can be more easily coerced.

A national identity system works against the interests of free people and a free society in several ways. One is by undercutting individuals' privacy. A widely used identification system makes the collection of identity information easier and more economical. Under a national ID, governmental and corporate bodies would collect more records of people's actions and movements. Whether directly or by inference, that would needlessly expose people's relationships, business activities, political leanings, social life, sexuality, and more.

This is not just a question of feelings about privacy or exposure. National ID systems shift power from individuals to institutions. They do provide genuine benefits, but extensive databases of personal information also render people more susceptible to the influence or control of data holders.

A national ID system would also place extraordinary power with the issuer of cards or the controller of the system. If showing ID is a gating function for access to goods, services, and infrastructure, then denying someone an ID allows the issuer to control access to those things. In a national ID system, the ID issuer can condition ID—and thus access to society—on obeying its commands.

Weaving Together a National ID

One might be inclined to think that U.S. state programs cannot create a national ID system. They can. It is national uniformity in data elements, not a national program, that constitutes a national ID system, with all its concerning effects. That is the first element of a national ID: use at a national scale.

The second hallmark of a national ID is that its possession or use is either practically or legally required. An identity card that everyone must carry is obviously a national ID card. A card or system that is one of many options for proving identity or other information is not a national ID; people can decline to use it and still easily access goods, services, or infrastructure. If law or regulation makes it very difficult to avoid carrying a card or using the system, then that puts the card or system into the national ID category. A system that automatically recognizes people presenting themselves in public, such as through facial recognition, is impossible to avoid and is thus practically required.

The final element of a national ID is that it is used for identification. This notion is fairly simple, but there are some subtleties. Identification occurs when a card or system shows that a physical person identified previously is the one appearing on later occasions. A national identifier like the Social Security number is not a full-fledged identification system. The Social Security number correlates names and numbers without making a biometric tie between the number and a physical person.

A variety of state programs threatens to produce a national ID, including facial recognition systems, license plate readers, and state participation in the federal government's Next Generation Identification (NGI) program. State mandates to use "E-Verify" and the "RIDE" (Records and Information from Department of Motor Vehicles for E-Verify) information-sharing program also advance the cause of national identification.

Facial recognition systems have become a popular purchase for departments of motor vehicles (DMVs) across the country. The benefit of suppressing identity fraud among driver's license applicants is offset, though, by the fact that DMVs are collecting digital images of each face. In the near future, these images may be used to identify people, and thus track them, using the camera systems that are increasingly networked across cities and towns. In similar fashion, license plate readers, which are being used in many jurisdictions for law enforcement purposes, also produce records of the movement of every car. By strong inference, that creates records of the movements of every driver.

Several states have signed memoranda of understanding (MOUs) with the Federal Bureau of Investigation (FBI) for the purpose of participating in the so-called Next Generation Identification initiative. The NGI's ostensible goal is to expand the capabilities of the Integrated Automated Fingerprint Identification System, the FBI's national fingerprint check system, by integrating additional biometrics such as facial imaging, palm

prints, and iris scans. The enhanced system serves a legitimate purpose in law enforcement, and the NGI is designed to expand its capabilities. But like other such systems, it may one day be used as a national identity repository, housing identity data on all Americans.

In the absence of federal immigration reform, a number of states have mandated the use of the E-Verify program by businesses and government contractors in their state. E-Verify checks the information supplied by new employees against federal government databases. The program is already beginning to integrate photos and state data about licensed drivers; its trajectory is to create a national ID that allows the government to perform background checks not just on every new worker, but conceivably on everyone seeking health care or picking up a prescription, cashing a check, using a credit card, applying for rental housing or a home purchase, buying a gun or ammunition, and so on. States participating in the RIDE program share data about their drivers with the federal E-Verify system so it can be part of new workers' background checks.

Creating an accurate and reliable system for verifying employment eligibility under the current immigration laws would require a national identification system, costing about $20 billion to create and hundreds of millions more per year to operate. Immigration reform legislation considered in summer 2007 would have required *all* Americans to have a so-called REAL ID card to get work (see below). This demonstrates the tight link between internal enforcement of immigration law and national ID proposals.

Whether assembled separately, one piece at a time, by states complying with federal dictates or seeking minor security gains, or assembled in one act by the federal government, the end-point of these efforts is a single system for tracking and control: a national ID. The most explicit effort to create a national ID thus far is the REAL ID program.

The REAL ID Program

In the wake of the terrorist attacks on 9/11, the idea of a national ID system gained currency. Among many interest groups and organizations poring over the problem of terrorism was a group called the Markle Foundation Task Force on National Security in the Information Age. One of the task force's reports contained an appendix titled "Reliable Identification for Homeland Protection and Collateral Gains," which endorsed a national ID system. That recommendation was cited in a short section of the 9/11 Commission's final report to support the assertion

that the federal government should take steps to secure the country's identity systems. Congress passed legislation responsive to this part of the 9/11 Commission Report in 2004's Intelligence Reform and Terrorism Prevention Act.

The following year, Congress passed the REAL ID Act without a hearing in either the House or the Senate by attaching it to a military spending bill. REAL ID repealed the earlier-passed legislation on identity security, attempting to create a national ID system instead. REAL ID seeks to coerce states into issuing their driver's licenses and identification cards according to national standards and requirements, including distinguishing between citizens and noncitizens. And it requires states to share driver information nationwide through a network of databases. REAL ID threatens to refuse the residents of noncompliant states at Transportation Security Administration (TSA) airport checkpoints when they go to travel.

Given the many defects of the REAL ID Act, state legislatures across the country originally passed resolutions and legislation objecting to the law or outright barring their own implementation of the act's provisions. When the original May 2008 compliance deadline approached, the Department of Homeland Security gave deadline extensions to states just for the asking. It even gave extensions to states that didn't ask for them, states whose leaders went out of their way to thumb their noses at the department. But in the years since REAL ID's passage, the Department of Homeland Security has worked to erode state resistance to the program. Many states continue to move toward REAL ID compliance in fits and starts.

Implementation of REAL ID would provide negligible national security gains at a significant cost in terms of personal privacy, power, and heightened risk of identity fraud. While state leaders resist implementation, Congress should spend no more funds on implementing REAL ID and should repeal the REAL ID Act.

Diverse and Competitive Private Identification and Credentialing

Rather than focus on government-issued ID cards, federal and state policy should encourage and foster the variety of identification and credentialing systems in the private marketplace today, as well as those that can be developed. People carry many types of privately issued identification cards and credentials that provide as good or greater security and identity assurance than government-issued cards. For example, many people carry credit cards that allow them to pay for goods or services securely. A variety

of privately issued access cards and devices, including phones, allow people entry to buildings or access to automobiles, health care, and so on.

State and federal governments should not insist on particular issuers' cards (i.e., their own government-issued ID). Instead, they should accept (and allow acceptance of) any card or device that provides sufficient proof of the information necessary for a given transaction. For example, many state laws require people buying alcohol to be at least 21 years old. But they don't allow just any sufficient proof of age; they require presentment of government-issued ID, including all the data that are extraneous to proving a person's age, including name, address, weight, eye color, and so on. As cards are scanned more and more often, these policies will needlessly cause tracking of law-abiding citizens that degrades their privacy.

In a marketplace for identification services, consumers should be able to choose which methods they use to identify themselves or prove relevant credentials like age; how much information they share for this purpose; and whether records of their activities are kept. Having a national ID would tend to deprive Americans of such choices.

Suggested Readings

Harper, Jim. "Alaska Biometrics." Testimony before the Health and Social Services Committee, Alaska House of Representatives, on S.B. 98, Biometric Information for ID, March 27, 2012.

———. "Electronic Employment Eligibility Verification: Franz Kafka's Solution to Illegal Immigration." Cato Institute Policy Analysis no. 612, March 6, 2008.

———. *Identity Crisis: How Identification Is Overused and Misunderstood*. Washington: Cato Institute, 2006.

———. "REAL ID: A State-by-State Update." Cato Institute Policy Analysis no. 749, May 12, 2014.

Nowrasteh, Alex, and Jim Harper. "Checking E-Verify: The Costs and Consequences of a National Worker Screening Mandate." Cato Institute Policy Analysis no. 775, July 7, 2015.

Weigel, David. "Who Killed REAL ID?" *Reason*, October 2008.

—Prepared by Jim Harper