

Checking Terrorists at the Door

Small Hopes for The Real ID Act

On May 11, 2005, President Bush signed into law an \$82 billion spending bill to provide more money for American troops in Afghanistan and Iraq. Attached to the bill was a controversial bit of legislation called the “Real ID Act,” a pet project of Representative James Sensenbrenner, a Wisconsin Republican and the chairman of the House Judiciary Committee. Among other things, the act requires that driver’s

licenses get a high-tech upgrade, and that states start demanding proof of legal residence and citizenship when an individual applies for a driver’s license.

Writing in *USA Today*, Sensenbrenner noted that the 9/11 terrorists used valid state driver’s licenses to board the airplanes they hijacked. He argued that the Real ID Act would require all states “to confirm the identities of applicants, confirm that visas are valid for foreign visitors, keep

accurate records, and make driver's licenses and ID cards extremely difficult to counterfeit." Such safeguards, Sensenbrenner wrote, will "prevent the next Mohammed Atta from using his six-month visa to obtain a six-year driver's license by requiring that a foreign visitor's license term ends when the visa expires."

Whether or not the Act will thwart the next Atta, it will create a large bureaucratic challenge for the states. As technology writer and privacy advocate Declan McCullagh has observed, "Practically speaking, your driver's license likely will have to be reissued to meet federal standards," a possibility that anyone who has wasted half a morning navigating the interminable lines of a state motor vehicles department might contemplate with horror. Sensenbrenner agrees that long lines and slow service will be a problem at first, but argues that "once these reforms are in place with more complete state records, license renewals should be faster and lines shorter."

The original impetus for the Real ID Act came from the final report of the 9/11 Commission, released last summer, which included recommendations for federally standardizing birth certificates, driver's licenses, and other forms of identification. "Fraud in identification documents is no longer just a problem of theft," the report concluded. "At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check

whether they are terrorists." Congress implemented some of the commission's recommendations in last year's Intelligence Reform and Terrorism Prevention Act, which changed the requirements for passports, pilot and driver's licenses, birth certificates, and other forms of identification. The 2005 Real ID Act includes a number of provisions that were stripped from last year's bill—including controversial measures relating to illegal immigrants and the new, more stringent requirements for driver's licenses.

Like most new federal mandates directed at the states, the Real ID Act will come with a price-tag that state governments, not the federal government, will have to pay. The Congressional Budget Office estimates a cost, over five years, of \$100 million; others claim the changes will end up costing states between \$500 and 700 million. Speaking to National Public Radio about the expense, Mike Huckabee, the Republican governor of Arkansas, did not mince words. "Once again," he said, "Congress has stuck it to the states. I mean, that's it in a nutshell. They don't have the courage to put forth a national ID system which they believe that we need, so what they're going to do is to hand not only the responsibility but also the burden of paying for it over to states already strapped by unfunded mandates like increases in Medicaid obligations and a host of things."

Some critics point to the many technical and bureaucratic challenges to implementing the Real ID Act, such as

verifying the forms of identification presented to DMV offices. “What’s the clerk in Denver supposed to do when someone provides a birth certificate from Angola?” asked Marc Rotenberg, the executive director of the Electronic Privacy Information Center, in a *Wired News* article. “Are they supposed [to call Angola] to check the accuracy of that?” And while licenses in most states already use the sort of “physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes” that the new act requires, they will now also have to incorporate “common machine-readable technology, with defined minimum data elements.”

Many privacy activists worry that that reference to “machine-readable technology” is a first step toward more invasive forms of citizen tracking and that it will end up giving private information to entities other than the government. “Everyone from 7-Eleven to the owner of your apartment building to a retailer and a bank are going to demand to see” your new driver’s license, Barry Steinhardt of the American Civil Liberties Union told *Wired News*. “And they’re going to be able to read all of the private data off of the machine-readable strip.” According to security guru Bruce Schneier, the “machine-readable technology” will “make identity theft easier” because “this information will be collected by bars and other businesses, and... will be resold to [database aggregator and reseller] companies like ChoicePoint and Acxiom. It actu-

ally doesn’t matter how well the states and federal government protect the data on driver’s licenses, as there will be parallel commercial databases with the same information.” Critics worry that driver’s licenses may eventually be required to have RFID tags—the tiny chips that can store a great deal more information than the magnetic strips currently used on some licenses, but which also have the potential to track individuals.

Supporters and opponents of the act disagree about whether the new license requirements constitute a backdoor way of introducing a national ID system. One of the act’s supporters, Representative Bob Goodlatte (a Republican from Virginia with a long history of work on information privacy issues), has denied it: “This is by no means a national ID card.” But Steinhardt says “this is a national ID, there’s no question about that.... It may be issued by the fifty states, but it’s going to be the same documents, which will be backed up by a huge database.” And as the country’s experience with Social Security numbers revealed, efforts to limit the use of such government-authorized identifiers are rarely successful.

These privacy concerns should not be taken lightly. But the Real ID Act’s ultimate flaw isn’t its potential implications for privacy; it is that the act perpetuates the notion that identification cards will necessarily improve security. Even with increased scrutiny of applicants for driver’s licenses, and even with government-run databases

backing up the new system, the driver's licenses of tomorrow will likely remain forgeable and obtainable under fake names. (The hijackers on September 11 used a combination of valid IDs, fake IDs, and real IDs that were obtained under fake names.)

Perhaps the new system will offer a marginal deterrent to lawbreakers—though at significant cost to states (in

money) and citizens (in wasted time). But we are frankly skeptical that the most committed and clever terrorists will be prevented from carrying out their nasty schemes by creating a quasi-national ID system for bouncing troublemakers at the door. As ever, only time will tell—and this is one case where we certainly hope we are wrong.