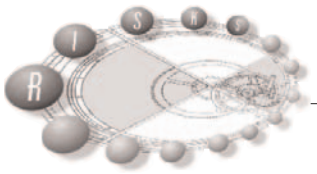

Real ID, Real Trouble?

According to the report of the 9/11 Commission, all but one of the 9/11 hijackers acquired some form of U.S. identification, some by fraud. Acquisition of these forms of identification would have assisted them in boarding commercial flights, renting cars, and other activities. As a result, the Commission and some lawmakers concluded it was necessary for the federal government to set technical standards for the issuance of birth certificates and sources of identification, such as driver's licenses. The result was the Real ID Act of 2005.

The new law states that beginning in 2008, "a Federal agency may not accept, for any official purpose, a driver's license or identification card issued by a State to any person unless the State is meeting the requirements of this section." This means the Department of Homeland Security will issue the technical standards for the issuance of the state driver's license. The practical impact, as CNET explained, is that "Starting three years from now, if you live or work in the United States, you'll need a federally approved ID card to travel on an airplane, open a bank account, collect Social Security payments, or take advantage of nearly any government service." And even some of the more conservative commentators in the U.S. have expressed concerns about "mission creep."

Several objections have been raised about the plan, including privacy and cost, but the most significant concern may be security. As Bruce Schneier has explained, "The biggest risk of a national ID system is the database. Any national ID card assumes the existence of a national database…large databases always have errors and outdated information." Even if the identity documents are maintained in the states, problems are likely.

One example concerns the vulnerability of the state agencies that collect the personal information used to produce the license. In 2005, the burglary of a Las Vegas Department of Motor Vehicles put thousands of driver's license holders at risk for identity theft. The information of at least 8,738 license and ID card holders was stolen, and reports of identity theft have already surfaced. Another report uncovered 10 "license-for-bribe" schemes in state DMVs in 2004.

PAUL WATSON

Not surprisingly, the administrators of the state license systems are among those most concerned about the proposal. As the director of Driver Services in Iowa said, "It's one thing to present a document; it's another thing to accept the document as valid. Verifying digital record information is going to be difficult." The National Conference of State Legislatures was more emphatic, "The Real ID Act would cause chaos and backlogs in thousands of state offices across the country, making the nation less secure."

The National Academy of Sciences anticipated many of these challenges in 2002, stating that the U.S. should carefully consider the goals of nationwide ID system: "The goals of a nationwide identification system should be clarified before any proposal moves forward. Proposals should be subject to strict public scrutiny and a thorough engineering review, because the social and economic costs of fixing an ID system after it is in place would be enormous."

The problems of building reliable systems for identification are not unique to the U.S. Many countries are confronting similar questions. In Great Britain, a national debate continues about the creation of a new identity card. The government contends the card is essential for combating crime, illegal immigration, and identity theft, and can be achieved for an operating cost of 584 million pounds per year. But a report from the London School of Economics challenged a number of the government positions and a subsequent report found further problems with the ID plan.

The U.K. group concluded, "ID requirements may actually make matters worse." The LSE report cited a recent high-profile breach: "Even as cards are promised to be more secure, attacks become much more sophisticated. Most recently, Russian security agents arrested policemen and civilians suspected of forging Kremlin security passes that guaranteed entrance to President Vladimir Putin's offices."

Systems of identification remain central to many forms of security. But designing secure systems that do not introduce new risks is proving more difficult than many policymakers had imagined. Perhaps it's time for the proponents of expanded identification systems to adopt the cautionary line from Hippocrates: "First, do no harm." C

MARC ROTENBERG (rotenberg@epic.org) is executive director of the Electronic Privacy Information Center (EPIC) and the former director of the ACM Washington Office; an expanded version of this column appears at www.epic.org.