

<http://www.latimes.com/news/local/la-me-realid20feb20,1,3044517.story>

From the Los Angeles Times

Plan for ID Cards Drawing Criticism

The new technology, required by law, hikes costs and raises risks of identity theft, some say.

By Evan Halper

Times Staff Writer

February 20, 2006

SACRAMENTO — When Congress rushed passage of the Real ID Act last spring, the idea was to foil terrorists.

States would be required to replace their current drivers' licenses with forgery-proof identification cards embedded with private information that government agents anywhere in the country could quickly scan to verify a person's identity.

"Americans have a right to know who is in their country, that people are who they say they are and that the name on the driver's license is the holder's real name, not some alias," House Judiciary Committee Chairman F. James Sensenbrenner Jr. (R-Wisconsin) said during a floor speech.

But as state legislators around the country now struggle to implement the law by a May 2008 deadline, many say it is highly problematic.

Officials in California say that meeting federal requirements could cost the state hundreds of millions of dollars, and that it could also increase identity theft and lead to invasions of privacy. The act is "a man-made disaster," said state Senate leader Don Perata (D-Oakland).

The state Senate will hold hearings starting Tuesday to examine, among other things, how much implementing the act will cost the state. Congress appropriated \$100 million to put the system in place nationwide. But the National Conference of State Legislatures has put the total price tag for states between \$9 billion and \$13 billion.

"This thing is such a big mess it is difficult to quantify at this point," said Sen. Michael Machado (D-Linden), who will oversee the hearings.

The obstacles to getting the system up and running here are enormous. Computer systems at the state Department of Motor Vehicles are so old that only a few state employees understand the language they run on, and the system is unsuited to handle the additional data storage mandated by the new law.

Officials also say that the law's requirements that documents be authenticated before licenses are issued could be particularly problematic in California, where many residents were born in other countries.

And even if those obstacles are overcome, security experts say, technology being considered for use in the cards could allow thieves with hand-held devices to steal the information on them from up to 20 feet away.

"This is just bad news all around," said David Williams, vice president for policy of Citizens Against Government Waste in Washington, D.C. "It is one of the biggest unfunded mandates the federal government has put on the states. It is a waste of money. And it is a potential invasion of privacy."

The federal government has yet to draft regulations for the program that would dictate what kind of technology states must use. But privacy advocates are particularly concerned about one option being considered, Radio Frequency Identification Technology, in which an embedded microchip contains information that can be read with a scanner. The technology is widely used in government and business, for such things as package tracking and the Fastrak highway toll collection system.

A diverse coalition of groups is sounding the alarm against using the technology to embed personal information into drivers' licenses. Last month, the American Civil Liberties Union, Americans for Tax Reform, American Conservative Union, National Lawyers Guild, Gun Owners of America and others sent a letter to the U.S. Department of Homeland Security speaking against using it.

"Mandating drastic change to new unproven technologies might actually weaken the security of citizens," they wrote.

The U.S. Government Accountability Office reported in June that the technology to block the signal from being inadvertently transmitted "has not yet been fully developed."

The government's planned use of the chips on U.S. passports, scheduled to start by the end of the year, has prompted a swell of panic from business travelers.

A Dutch security firm demonstrated on live television this month how hackers could easily mine the personal data from a prototype Dutch passport embedded with such a chip.

The GAO report, meanwhile, noted that misuse of the data is not limited to criminals. For instance, the government could place scanners in public places to track movements of citizens. The report says the chip could also be used to create profiles that "ascertain something about the individual's habits, tastes or predilections."

"Both profiling and tracking can compromise an individual's privacy and anonymity," the

report said.

The state Senate passed a bill that would ban the placement of these chips on government-issued identification for three years, to give the government time to develop better ways to mitigate the security and privacy issues the technology presents.

But the law, even if passed by the Assembly later this year, will be moot if the federal government ultimately decides to go with the technology. Bill author Sen. Joe Simitian (D-Palo Alto), said he hopes his legislation will at least force a "wider ranging discussion about these privacy implications."

A spokesman for the Department of Homeland Security said the agency is taking such concerns into consideration, but that it has not rejected requiring the technology in drivers' licenses.

Even if the chips are scrapped, activists warn that identity theft is still a major concern. Tens of thousands of DMV agents, airport security guards, and state and local bureaucrats will have access to all the personal information embedded in cards, as well as a national database with scanned images of personal documents that could include Social Security cards, passports and birth certificates.

"The goal is to catch bad guys, but you are catching good guys," said Bruce Schneier, founder of Counterpane Internet Security, an international data security firm.

Sacramento has a long history of computer debacles. State officials spent \$51 million trying to install a new computer system at the DMV in the mid-1990s before abandoning the project altogether. A few years later the state pulled the plug on a computer system to track fathers who didn't pay child support, after dumping \$100 million into that project.

In 2002, there was the Oracle software scandal, in which state officials signed a \$95-million contract with the politically connected company for services that a state audit found were largely unneeded. The contract was ultimately canceled.

The Real ID Act, meanwhile, has already claimed its first political casualty in Sacramento.

In September, the state Senate did not confirm the appointment of Joan Borucki, Gov. Arnold Schwarzenegger's nominee to head the DMV, after she failed to convince legislators she would be able to effectively negotiate with Washington on the law's requirements.

In testimony before the Legislature, she was not optimistic about California's ability to handle the new mandates, describing the DMV computer system as a "bowl of tangled spaghetti of code and programming."

"There are very few people left in department who even know what was embedded in that code," Borucki said.

If you want other stories on this topic, search the Archives at latimes.com/archives.

TMSReprints

Article licensing and reprint options

Copyright 2006 Los Angeles Times | [Privacy Policy](#) | [Terms of Service](#)
[Home Delivery](#) | [Advertise](#) | [Archives](#) | [Contact](#) | [Site Map](#) | [Help](#)