Resolved: "Federally standardized, electronically readable driver's licenses & ID cards, and their associated federal database, should be implemented throughout the United States."

CNET NEWS.COM

National ID cards on the way?

By Declan McCullagh

A recent vote in Congress endorsing standardized, electronically readable driver's licenses has raised fears about whether the proposal would usher in what amounts to a national ID card.

In a vote that largely divided along party lines, the U.S. House of Representatives approved a Republican-backed measure that would compel states to design their driver's licenses by 2008 to comply with federal antiterrorist standards. Federal employees would reject licenses or identity cards that don't comply, which could curb Americans' access to everything from airplanes to national parks and some courthouses.

The congressional maneuvering takes place as governments are growing more interested in implanting technology in ID cards to make them smarter and more secure. The U.S. State Department soon will begin issuing passports with radio frequency identification, or RFID, chips embedded in them, and Virginia may become *the first state to glue RFID* tags into all its driver's licenses.

Proponents of the Real ID Act say it's needed to frustrate both terrorists and illegal immigrants. Critics say it imposes more requirements for identity documents on states, and gives the Department of Homeland Security carte blanche to do nearly anything else "to protect the national security interests of the United States."

"Supporters claim it is not a national ID because it is voluntary," Rep. Ron Paul of Texas, one of the eight Republicans to object to the measure, said during the floor debate this week. "However, any state that opts out will automatically make nonpersons out of its citizens. They will not be able to fly or to take a train."

Paul warned that the legislation, called the Real ID Act, gives unfettered authority to the Department of Homeland Security to design state ID cards and driver's licenses. Among the possibilities: biometric information such as retinal scans, fingerprints, DNA data and RFID tracking technology.

Proponents of the Real ID Act say it adheres to the recommendations of the 9/11 Commission and is needed to frustrate both terrorists and illegal immigrants. Only a portion of the legislation regulates ID cards; the rest deals with immigration law and asylum requests. "American citizens have the 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 real holder's name, not some alias," F. James Sensenbrenner, R-Wisc., said last week.

"If these commonsense reforms had been in place in 2001, they would have hindered the efforts of the 9/11 terrorists, and they will go a long way toward helping us prevent another tragedy like 9/11," said House Majority Leader Tom DeLay, R-Texas.

Now the Real ID Act heads to the Senate, where its future is less certain. Senate rules make it easier for politicians to derail legislation, and an aide said Friday that Sen. Patrick Leahy, the top Democrat on the Judiciary Committee, was concerned about portions of the bill.

Sen. Dianne Feinstein of California, the top Democrat on a terrorism subcommittee, said "I basically support the thrust of the bill" in an e-mail to CNET News.com on Friday. "The federal government should have the ability to issue standards that all driver's licenses and identification documents should meet."

"Spy-D" cards?

National ID cards are nothing new, of course. Many European, Asian and South American countries require their citizens to carry such documents at all times, with legal punishments in place for people caught without them. Other nations that share the English common law tradition, including Australia and New Zealand, have rejected such schemes.

Conservatives and libertarians typically argue that a national ID card will increase the power of the government, and they fear the dehumanizing effects of laws enacted as a result. Civil liberties groups tend to worry about the administrative problems, the opportunities for criminal mischief, and the potential irreversibility of such a system.

Those long-standing concerns have become more pointed recently, thanks to the opportunity for greater tracking--as well as potentially greater security for ID documents--that technologies such as RFID provide. Though the Real ID act does not specify RFID or biometric technology, it requires that the Department of Homeland Security adopt "machine-readable technology" standards and provides broad discretion in how to do it.

An ad hoc alliance of privacy groups and technologists recently has been fighting proposals from the International Civil Aviation Organization to require that passports and other travel documents be outfitted with biometrics and remotely readable RFID-type "contact-less integrated circuits."

The ICAO, a United Nations organization, argues the measures are necessary to reduce fraud, combat terrorism and improve airline security. But its critics have raised questions about how the technology could be misused by identity thieves with RFID readers, and they say it would "promote irresponsible national behavior."

In the United States, the federal government is planning to embed RFID chips in all U.S. passports and some foreign visitor's documents. The U.S. State Department is now evaluating so-called e-passport technology from eight different companies. The agency plans to select a supplier and issue the first e-passports this spring, starting in Los Angeles, and predicts that all U.S. passport agencies will be issuing them within a year.

The high-tech passports are supposed to deter theft and forgeries, as well as accelerate immigration checks at airports and borders. They'll contain within their covers a miniscule microchip that stores basic data, including the passport holder's name, date of birth and place of birth. The chip, which can transmit information through a tiny included antenna, also has enough room to store biometric data such as digitized fingerprints, photographs and iris scans.

Border officials can compare the information on the chip to that on the rest of the passport and to the person actually carrying it. Discrepancies could signal foul play.

In a separate program, the Department of Homeland Security plans to issue RFID devices to foreign visitors that enter the country at the Mexican and Canadian borders. The agency plans to start a yearlong test of the technology in July at checkpoints in Arizona, New York and Washington state.

The idea is to aid immigration officials in tracking visitors' arrivals and departures and snare those who overstay their visas. Similar to e-passports, the new system should speed up inspection procedures. It's part of the US-VISIT program, a federal initiative designed to capture and share data such as fingerprints and photographs of foreign visitors.

A "Trojan horse"

The legislation approved by the House last Thursday follows a related measure President Bush signed into law in December. That law gives the Transportation Department two years to devise standard rules for state licenses, requires information to be stored in "machine-readable" format, and says noncompliant ID cards won't be accepted by federal agencies.

But critics fret that the new bill goes even further. It shifts authority to the Department of Homeland Security, imposes more requirements for identity documents on states, and gives the department carte blanche to do nearly anything else "to protect the national security interests of the United States."

"In reality, this bill is a Trojan horse," said Paul, the Republican congressman. "It pretends to offer desperately needed border control in order to stampede Americans into sacrificing what is uniquely American: our constitutionally protected liberty."

Unlike last year's measure, the Real ID Act "doesn't even mention the word 'privacy,'" said Marv Johnson, a lobbyist for the American Civil Liberties Union.

Another section of the Real ID Act that has raised alarms is the linking of state Department of Motor Vehicles databases, which was not part of last year's law. Among the information that must be shared: "All data fields printed on drivers' licenses and identification cards" and complete drivers' histories, including motor vehicle violations, suspensions and points on licenses.

Some senators have indicated they may rewrite part of the measure once they begin deliberations.

Sen. Jon Kyl, R-Ariz., chairman of a terrorism subcommittee, is readying his own bill that will be introduced within a few weeks, spokesman Andrew Wilder said on Friday. "He has been at work on his own version of things," Wilder said. "Senator Kyl does support biometric identifiers."

MSNBC.com

Where rubber meets the road in privacy debate

New federal requirements for driver's licenses rev up the arguments

By Mike Stuckey
Senior news editor
MSNBC

Updated: 5:22 a.m. ET Oct. 20, 2006

Any hope we may have of keeping government, industry and criminals out of our personal business is scheduled to vanish completely in 18 months, privacy advocates say.

That's when the federal government's Real ID Act is to be fully in place, effectively setting up a national identification program by requiring states to adopt strict new high-tech standards for driver's licenses and ID cards if they are to be accepted by federal authorities at places ranging from airports to U.S. courthouses.

The act's passage last year has crystallized the U.S. debate over the delicate balance between individual privacy rights and the government's desire to securely identify travelers, applicants for federal benefits and anyone else who may pose a threat to its security or economy..

Real ID's looming implementation has fueled sky-is-falling rhetoric from a broad spectrum of groups. They say it will push the United States firmly toward an Orwellian surveillance society in which the federal government can track our every move. The personal data of every American with a driver's license or state ID card also will be far easier for businesses and criminals to obtain, cost billions to implement and do very little to fulfill its stated aim of increasing homeland security, they maintain.

"It is a very large step toward a national-identification, you-have-to-have-your-papers type of world," said Melissa Ngo, staff counsel of the Electronic Privacy Information Center.

On the other side, backers of Real ID say the technology is essential for government officials in the post-9/11 world to know who's who. And security industry representatives say that the technology itself and policy decisions on how it's implemented will do a fine job of protecting privacy, and could even enhance it.

Just what the 9/11 Commission ordered

“The Real ID Act is a direct implementation of one of the 9/11 Commission recommendations,” said Jeff Lungren, spokesman for House Judiciary Chairman Rep. James Sensenbrenner, R-Wisc., the legislation's key sponsor. “There's a ton of misconceptions that have been promulgated by the opponents from the get-go. It's unfortunate that they're continuing to do so.”

The thinking behind Real ID is that since the 9/11 hijackers were allowed through airport security with legitimate state-issued driver's licenses or ID cards, the standards that states use to grant the cards must be tightened. Those standards are spelled out in a 1,767-word section of the act and require, in addition to the holder's name, gender, date of birth and residential address, a digital photograph, “physical security features” to prevent fraud, and the ability to be accessed by “machine-readable technology.”

But it's what lies beneath those features that raises the specter of Big Brother for privacy advocates and budget concerns for state governments. In what some critics see as an unvarnished bid to also control illegal immigration, the act requires that states go to extraordinary lengths to verify the identities of people to whom they issue cards, ensuring that cardholders are in the country legally and verifying their Social Security numbers. The states must keep this proof on file for seven to 10 years, and they must maintain a database with all driver's license information that can be accessed by all the other states. The act also bars drivers from holding a license in more than one state at a time.

Precisely how the language of the Real ID Act is to be carried out at the practical level is in the hands of the Department of Homeland Security, which is in “the process of developing the draft regulations,” according to DHS spokesman Jarrod Agen. “The best timeline I can give is that we should have those out for public comment by the end of the year.” States are antsy to see the rules because the law calls for the new licenses to be issued as of May 11, 2008, which doesn't leave a lot of time for the major changes that will be required in some DMVs.

Other measures on the table

Although Real ID is getting the most attention right now in the privacy-vs.-security debate, it's just one of a host of U.S. and international moves aimed at increasing security in the wake of the 2001 terrorist attacks. Others, including high-tech passports and the Western Hemisphere Travel Initiative, which tightens ID requirements for travel between the United States and other nations in the region, have fueled similar arguments over the proper use of technology for such programs, as has a massive plan to create a single ID for federal employees and contractors to access both buildings and computer networks.

"There's a mess," said Jim Harper of the Cato Institute. "Congress was stampeded into passing a whole raft of 9/11 initiatives. ... This is all part of what I think is a collective overreaction to the terrorist threat." Harper was speaking at a recent press conference to blast the Western Hemisphere proposal. But he just as easily could have been railing against the Real ID Act, which he did a day earlier in an interview with MSNBC.com.

Harper, Cato's director of information policy studies and author of "Identity Crisis: How Identification is Overused and Misunderstood," is arguably the staunchest critic of Real ID on privacy grounds.

"The average person does not see the privacy consequence," Harper said. "The one that I prioritize the most is the likelihood that Real ID will be used for tracking and surveillance. That's not an immediate concern but down the line you can be sure it will used that way."

Harper and other foes of Real ID fear that its potential for misuse rests chiefly in the combination of "machine readable" technology and the linking of state databases.

"Machine readable" technology suggests the use of Radio Frequency Identification chips or a similar technology, which critics like Chris Calabrese of the American Civil Liberties Union say open up whole new horizons for fraud and abuse. Because the chips emit radio signals that can be read at a distance, the possibility exists for them to be read by criminals and the data used for nefarious means, said Calabrese, counsel to the ACLU's Technology and Liberty Program. He also has no doubt that commercial users will capitalize on the neat data package, gleaning and storing personal data much more easily than they can now when a driver's license is part of a business transaction.

Real ID proponents and tech industry representatives say such fears are overblown. First, they say, true RFID chips that were made for simple tasks like tracking cattle and retail merchandise can transmit their signals 30 feet or more and should not be used in ID card systems. Rather, ID card reading systems would use "contactless security controllers," said Joerg Borchert, a California-based official with Infineon Technologies. The German company is supplying such chips to the U.S. State Department for use in new "e-passports" that some U.S. travelers began receiving in August.

'A little tiny computer'

The passport chips are "basically a little tiny computer," Borchert said. "It can do computations like your PC," meaning that it can be programmed to be far more secure than a typical RFID chip, he explained. There is little risk of its signal being intercepted, he said, because the card needs to be held within three to four inches of a card reader to work.

Borchert's confidence in the chip technology and other high-tech features of identity cards was echoed by other industry representatives. Neville Pattinson of Gemalto, which along with Infineon is seeking part of the giant e-passport pie from the State Department, said his firm currently does passport work for 11 nations. As to security breaches with "contactless" chips, there have been "none whatsoever."

Added Randy Vanderhoof, executive director of the industry's Smart Card Alliance, "This technology has been around for more than 20 years. There's a lot of good, solid data that shows that this technology works. Give it a chance."

Hacker's 'good media stunt'

Real ID opponents aren't buying it. "Any contactless chip is going to be problematic," said the ACLU's Calabrese. "Their purpose is to be read at a distance. It's like trying to make water less wet. ... Every day, the industry says, 'We've defeated all these problems' and at the next hacker conference someone shows otherwise."

Case in point: In August, Lukas Grunwald, a German security expert, showed how he could clone a chip in an e-passport at a Las Vegas conference. His feat was dismissed as an "opportunistic" ploy by Pattinson and a "non-issue" but a "good media stunt" by Borchert who say that merely being able to copy a chip is analogous to photocopying the document and doesn't compromise its security.

Grunwald told MSNBC.com that his critics missed a key point of his demonstration. Because an ID system would read a cloned chip, that means "the computer systems accept data from an untrusted data source," raising the possibility that "with some additional malware, this could infect the inspection system with a trojan, or attach and shut down the inspection system by making an alert on any passenger and suspecting him as a terrorist."

But Borchert denied that, saying the system would not activate or read the chip until the card passed three other security tests.

If you don't believe the bad guys can steal your data with high-tech trickery, you can be sure they'll get it in some other fashion, say Real ID's foes.

"Something this valuable, a database of every person in the country who wants a state ID or a driver's license would be just too tempting to criminals," said Ngo of the Electronic Privacy Information Center, adding that they will either hack the system or bribe state employees.

And commercial users also will be lining up to leverage the technology, said Calabrese. He snort-laughed at the notion that government policies will keep that from happening. "These protections for the most part don't exist." Industry has "a great incentive to have commercial use of this product."

But criminal or commercial misuse of Real ID cannot be blamed on the technology, said Vanderhoof. "There is no risk when it's implemented properly. ... What I object to is the assumption of guilt and the presumption of failure that some of the privacy advocates place on the technology, often because they don't understand how it is going to be implemented."

Scott Carr of Digimarc, whose equipment and services help produce 50 million of the 72 million driver's licenses issued each year in the United States, said his firm's technique of "digital watermarking" is a good example of "incredibly reliable" technology that can increase security for both license holders and those who check them.

By placing "bits of data into content in a way that you or I don't perceive it but a computer can read it," digital watermarking creates ID cards that can be checked with "without having to do a database lookup that might compromise your privacy," he said. As explained on Digimarc's Web site, the "watermarks" are "woven into the artwork of the secure ID" and "can easily be read by many commonly available document scanners equipped with special software."

'Technology isn't static'

Despite assurances by Carr and others, privacy advocates are convinced that technology will eventually fail. They say they're only basing their concerns on what has happened in the past. "That's just the nature of technology," said Ngo. "If you build something, someone else will be able to break into it. Then you can try to make it stronger, then someone else will be able to break into it. Technology isn't static, so we shouldn't act as if it is."

Those arguments aside, Real ID's foes believe they have an ace in the hole: The costs to states for retraining DMV employees, using computer chips, verifying documents and linking databases will be so enormous that the whole plan will collapse before it's implemented, predicted Cato's Harper. An estimate from state government organizations last month put the tab at $11 billion, more than 100 times the $100 million quoted by sponsor Sensenbrenner. The states say they simply don't have the money.

But Lungren, the Sensenbrenner spokesman, said the states have come up with "wild numbers. ... We don't know what DHS is going to require so how do they know what it's going to cost?"

Any cost is too much, Ngo said. "I want all the billions of dollars that are being spent on this Real ID program to be spent on more cops, more investigators for the FBI and the CIA ... and more people for air security."

Calabrese agreed, pointing out that simply "knowing who someone is just doesn't tell you whether or not someone's going to be a terrorist."

"That's just a really defeatist attitude," replied Lungren. "The terrorists didn't have bombs. They had box cutters and driver's licenses."