Chips in official IDs raise privacy fears

July 11 2009, By TODD LEWAN , AP National Writer

In this April 10, 2009. photo, Chris Paget, a self-described "ethical hacker," sits in the back of his car with electronic equipment seeking information from imbedded radio frequency identification, or RFID chips as people pass him along the Embarcadero in San Francisco. (AP Photo/Eric Risberg)

Climbing into his Volvo, outfitted with a Matrics antenna and a Motorola reader he'd bought on eBay for $190, Chris Paget cruised the streets of San Francisco with this objective: To read the identity cards of strangers, wirelessly, without ever leaving his car.

It took him 20 minutes to strike hacker's gold.

Zipping past Fisherman's Wharf, his scanner detected, then downloaded to his laptop, the unique serial numbers of two pedestrians' electronic U.S. passport cards embedded with radio frequency identification, or RFID, tags. Within an hour, he'd "skimmed" the identifiers of four more of the new, microchipped PASS cards from a distance of 20 feet.

Embedding identity documents - passports, drivers licenses, and the like - with RFID chips is a no-brainer to government officials. Increasingly, they are promoting it as a 21st century application of technology that will help speed border crossings, safeguard credentials against counterfeiters, and keep terrorists from sneaking into the country.

But Paget's February experiment demonstrated something privacy advocates had feared for years: That RFID, coupled with other technologies, could make people trackable without their knowledge or consent.

He filmed his drive-by heist, and soon his video went viral on the Web, intensifying a debate over a push by government, federal and state, to put tracking technologies in identity documents and over their potential to erode privacy.

Putting a traceable RFID in every pocket has the potential to make everybody a blip on someone's radar screen, critics say, and to redefine Orwellian government snooping for the digital age.

"Little Brother," some are already calling it - even though elements of the global surveillance web they warn against exist only on drawing boards, neither available nor approved for use.

But with advances in tracking technologies coming at an ever-faster rate, critics say, it won't be long before governments could be able to identify and track anyone in real time, 24-7, from a cafe in Paris to the shores of California.

The key to getting such a system to work, these opponents say, is making sure everyone carries an RFID tag linked to a biometric data file.

On June 1, it became mandatory for Americans entering the United

States by land or sea from Canada, Mexico, Bermuda and the Caribbean to present identity documents embedded with RFID tags, though conventional passports remain valid until they expire.

Among new options are the chipped "e-passport," and the new, electronic PASS card - credit-card sized, with the bearer's digital photograph and a chip that can be scanned through a pocket, backpack or purse from 30 feet.

Alternatively, travelers can use "enhanced" driver's licenses embedded with RFID tags now being issued in some border states: Washington, Vermont, Michigan and New York. Texas and Arizona have entered into agreements with the federal government to offer chipped licenses, and the U.S. Department of Homeland Security has recommended expansion to non-border states. Kansas and Florida officials have received DHS briefings on the licenses, agency records show.

The purpose of using RFID is not to identify people, says Mary Ellen Callahan, the chief privacy officer at Homeland Security, but rather "to verify that the identification document holds valid information about you."

Likewise, U.S. border agents are "pinging" databases only to confirm that licenses aren't counterfeited. "They're not pulling up your speeding tickets," she says, or looking at personal information beyond what is on a passport.

The change is largely about speed and convenience, she says. An RFID document that doubles as a U.S. travel credential "only makes it easier to pull the right record fast enough, to make sure that the border flows, and is operational" - even though a 2005 Government Accountability Office report found that government RFID readers often failed to detect travelers' tags.

Such assurances don't persuade those who liken RFID-embedded documents to barcodes with antennas and contend they create risks to privacy that far outweigh the technology's heralded benefits. They warn it will actually enable identity thieves, stalkers and other criminals to commit "contactless" crimes against victims who won't immediately know they've been violated.

Neville Pattinson, vice president for government affairs at Gemalto, Inc., a major supplier of microchipped cards, is no RFID basher. He's a board member of the Smart Card Alliance, an RFID industry group, and is serving on the Department of Homeland Security's Data Privacy and Integrity Advisory Committee.

Still, Pattinson has sharply criticized the RFIDs in U.S. driver's licenses and passport cards. In a 2007 article for the Privacy Advisor, a newsletter for privacy professionals, he called them vulnerable "to attacks from hackers, identity thieves and possibly even terrorists."

RFID, he wrote, has a fundamental flaw: Each chip is built to faithfully transmit its unique identifier "in the clear, exposing the tag number to interception during the wireless communication."

Once a tag number is intercepted, "it is relatively easy to directly associate it with an individual," he says. "If this is done, then it is possible to make an entire set of movements posing as somebody else without that person's knowledge."

Echoing these concerns were the AeA - the lobbying association for technology firms - the Smart Card Alliance, the Institute of Electrical and Electronics Engineers, the Business Travel Coalition, and the Association of Corporate Travel Executives.

Meanwhile, Homeland Security has been promoting broad use of RFID

even though its own advisory committee on data integrity and privacy warned that radio-tagged IDs have the potential to allow "widespread surveillance of individuals" without their knowledge or consent.

In its 2006 draft report, the committee concluded that RFID "increases risks to personal privacy and security, with no commensurate benefit for performance or national security," and recommended that "RFID be disfavored for identifying and tracking human beings."

For now, chipped PASS cards and enhanced driver's licenses are optional and not yet widely deployed in the United States. To date, roughly 192,000 EDLs have been issued in Washington, Vermont, Michigan and New York.

But as more Americans carry them "you can bet that long-range tracking of people on a large scale will rise exponentially," says Paget, a self-described "ethical hacker" who works as an Internet security consultant.

Could RFID numbers eventually become de facto identifiers of Americans, like the Social Security number?

Such a day is not far off, warns Katherine Albrecht, a privacy advocate and co-author of "Spychips," a book that is sharply critical of the use of RFID in consumer items and official ID documents.

"There's a reason you don't wear your Social Security number across your T-shirt," Albrecht says, "and beaming out your new, national RFID number in a 30-foot radius would be far worse."

There are no federal laws against the surreptitious skimming of Americans' RFID numbers, so it won't be long before people seek to profit from this, says Bruce Schneier, an author and chief security officer at BT, the British telecommunications operator.

Data brokers that compile computer dossiers on millions of individuals from public records, credit applications and other sources "will certainly maintain databases of RFID numbers and associated people," he says. "They'd do a disservice to their stockholders if they didn't."

But Gigi Zenk, a spokeswoman for the Washington state Department of Licensing, says Americans "aren't that concerned about the RFID, particularly in this day and age when there are a lot of other ways to access personal information on people."

Tracking an individual is much easier through a cell phone, or a satellite tag embedded in a car, she says. "An RFID that contains no private information, just a randomly assigned number, is probably one of the least things to be concerned about, frankly."

Still, even some ardent RFID supporters recognize that these next-generation RFID cards raise prickly questions.

Mark Roberti, editor of RFID Journal, an industry newsletter, recently acknowledged that as the use of RFID in official documents grows, the potential for abuse increases.

"A government could do this, for instance, to track opponents," he wrote in an opinion piece discussing Paget's cloning experiment. "To date, this type of abuse has not occurred, but it could if governments fail to take privacy issues seriously."

Imagine this: Sensors triggered by radio waves instructing cameras to zero in on people carrying RFID, unblinkingly tracking their movements.

Unbelievable? Intrusive? Outrageous?

Actually, it happens every day and makes people smile - at the Alton Towers amusement park in Britain, which videotapes visitors who agree to wear RFID bracelets as they move about the facility, then sells the footage as a keepsake.

This application shows how the technology can be used effortlessly - and benignly. But critics, noting it can also be abused, say federal authorities in the United States didn't do enough from the start to address that risk.

The first U.S. identity document to be embedded with RFID was the "e-passport."

In the wake of the Sept. 11 attacks - and the finding that some of the terrorists entered the United States using phony passports - the State Department proposed mandating that Americans and foreign visitors carry "enhanced" passport booklets, with microchips embedded in the covers.

The chips, it announced, would store the holder's information from the data page, a biometric version of the bearer's photo, and receive special coding to prevent data from being altered.

In February 2005, when the State Department asked for public comment, it got an outcry: Of the 2,335 comments received, 98.5 percent were negative, with 86 percent expressing security or privacy concerns, the department reported in an October 2005 notice in the Federal Register.

"Identity theft was of grave concern," it stated, adding that "others expressed fears that the U.S. Government or other governments would use the chip to track and censor, intimidate or otherwise control or harm them."

It also noted that many Americans expressed worries "that the information could be read at distances in excess of 10 feet."

Those concerned citizens, it turns out, had cause.

According to department records obtained by researchers at the University of California, Berkeley, under a Freedom of Information Act request and reviewed by the AP, discussion about security concerns with the e-passport occurred as early as January 2003 but tests weren't ordered until the department began receiving public criticism two years later.

When the AP asked when testing was initiated, the State Department said only that "a battery of durability and electromagnetic tests were performed" by the National Institute of Standards and Technology, along with tests "to measure the ability of data on electronic passports to be surreptitiously skimmed or for communications with the chip reader to be eavesdropped," testing which "led to additional privacy controls being placed on U.S. electronic passports ... "

Indeed, in 2005, the department incorporated metallic fibers into the e-passport's front cover, since metal can reduce the range at which RFID can be read. Personal information in the chips was encrypted and a cryptographic "key" added, which required inspectors to optically scan the e-passport first for the chip to communicate wirelessly.

The department also announced it would test e-passports with select employees, before giving them to the public. "We wouldn't be issuing the passports to ourselves if we didn't think they're secure," said Frank Moss, deputy assistant Secretary of State for passport services, in a CNN interview.

But what of Americans' concerns about the e-passport's read range?

In its October 2005 Federal Register notice, the State Department reassured Americans that the e-passport's chip - the ISO 14443 tag - would emit radio waves only within a 4-inch radius, making it tougher to hack.

Technologists in Israel and England, however, soon found otherwise. In May 2006, at the University of Tel Aviv, researchers cobbled together $110 worth of parts from hobbyists kits and directly skimmed an encrypted tag from several feet away. At the University of Cambridge, a student showed that a transmission between an e-passport and a legitimate reader could be intercepted from 160 feet.

The State Department, according to its own records obtained under FOIA, was aware of the problem months before its Federal Register notice and more than a year before the e-passport was rolled out in August 2006.

"Do not claim that these chips can only be read at a distance of 10 cm (4 inches)," Moss wrote in an April 22, 2005, e-mail to Randy Vanderhoof, executive director of the Smart Card Alliance. "That really has been proven to be wrong."

The chips could be skimmed from a yard away, he added - all a hacker would need to read e-passport numbers, say, in an elevator or on a subway.

Other red flags went up. In February 2006, an encrypted Dutch e-passport was hacked on national television, with researchers gaining access to the document's digital photograph, fingerprint and personal data. Then British e-passports were hacked using a $500 reader and software written in less than 48 hours.

The State Department countered by saying European e-passports weren't

as safe as their American counterparts because they lacked the cryptographic key and the anti-skimming cover.

But recent studies have shown that more powerful readers can penetrate even the metal sheathing in the U.S. e-passport's cover.

John Brennan, a senior policy adviser at the State Department's Bureau of Consular Affairs, concedes it may be possible for a reader to overpower the e-passport's protective shield from a distance.

However, he adds, "you could not do this in any large-scale, concerted fashion without putting a bunch of infrastructure in place to make it happen. The practical vulnerabilities may be far less than some of the theoretical scenarios that people have put out there."

That thinking is flawed, says Lee Tien, a senior attorney and surveillance expert with the Electronic Frontier Foundation, which opposes RFID in identity documents.

It won't take a massive government project to build reader networks around the country, he says: They will grow organically, for commercial purposes, from convention centers to shopping malls, sports stadiums to college campuses. Federal agencies and law enforcement wouldn't have to control those networks; they already buy information about individuals from commercial data brokers.

"And remember," Tien adds, "technology always gets better ... "

With questions swirling around the e-passport's security, why then did the government roll out more RFID-tagged documents - the PASS card and enhanced driver's license, which provide less protection against

hackers?

The RFIDs in enhanced driver's licenses and PASS cards are nearly as slim as paper. Each contains a silicon computer chip attached to a wire antenna, which transmits a unique identifier via radio waves when "awakened" by an electromagnetic reader.

The technology they use is designed to track products through the supply chain. These chips, known as EPCglobal Gen 2, have no encryption, and minimal data protection features. They are intended to release their data to any inquiring Gen 2 reader within a 30-foot radius.

This might be appropriate when a supplier is tracking a shipment of toilet paper or dog food; but when personal information is at stake, privacy advocates ask: Is long-range readability truly desirable?

The departments of State and Homeland Security say remotely readable ID cards transmit only RFID numbers that correspond to records stored in government databases, which they say are secure. Even if a hacker were to copy an RFID number onto a blank tag and place it into a counterfeit ID, they say, the forger's face still wouldn't match the true cardholder's photo in the database, rendering it useless.

Still, computer experts such as Schneier say government databases can be hacked. Others worry about a day when hackers might deploy readers at "chokepoints," such as checkout lines, skim RFID numbers from people's driver's licenses, then pair those numbers to personal data skimmed from chipped credit cards (though credit cards are harder to skim). They imagine stalkers using skimmed RFID numbers to track their targets' comings and goings. They fear government agents will compile chip numbers at peace rallies, mosques or gun shows, simply by strolling through a crowd with a reader.

Others worry more about the linking of chips with other identification methods, including biometric technologies, such as facial recognition.

The International Civil Aviation Organization, the U.N. agency that sets global standards for passports, now calls for facial recognition in all scannable e-passports.

Should biometric technologies be coupled with RFID, "governments will have, for the first time in history, the means to identify, monitor and track citizens anywhere in the world in real time," says Mark Lerner, spokesman for the Constitutional Alliance, a network of nonprofit groups, lawmakers and citizens opposed to remotely readable identity and travel documents.

Implausible?

For now, perhaps. Radio tags in EDLs and passport cards can't be scanned miles away.

But scientists are working on technologies that might enable a satellite or a cell tower to scan a chip's contents. Critics also note advances in the sharpness of closed-circuit cameras, and point out they're increasingly ubiquitous. And more fingerprints, iris scans and digitized facial images are being stored in government databases. The FBI has announced plans to assemble the world's largest biometric database, nicknamed "Next Generation Identification."

"RFID's role is to make the collection and transmission of people's biometric data quick, easy and nonintrusive," says Lerner. "Think of it as the thread that ties together the surveillance package."

On the Net:

www.dhs.gov/xprevprot/programs … c_1200693579776.shtm

travel.state.gov/passport/eppt/eppt_2498.html

www.stoprealidcoalition.com/

www.smartcardalliance.org/page … /publications-realid

www.eff.org/deeplinks/2009/02/ … assports-scanned-car

epic.org/privacy/surveillance/spotlight/0907/