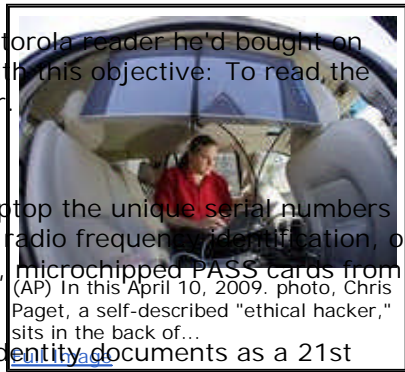


Climbing into his Volvo, outfitted with a Matrics antenna and a Motorola reader he'd bought on eBay for \$190, Chris Paget cruised the streets of San Francisco with this objective: To read the identity cards of strangers, wirelessly, without ever leaving his car.

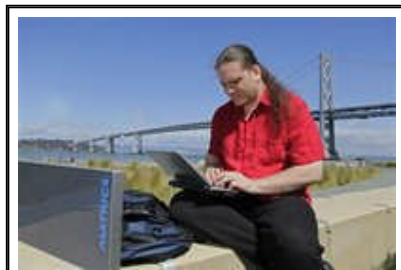
It took him 20 minutes to strike hacker's gold.

Zooming past Fisherman's Wharf, his scanner 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" four more of the new, microchipped PASS cards from a distance of 20 feet.



Increasingly, government officials are promoting the chipping of identity documents 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.

Google sponsored links



(AP) In this April 10, 2009, photo, Chris Paget, a self-described "ethical" hacker, sits with his... [Full Image](#)

But Paget's February experiment demonstrated something that privacy advocates had feared for years: The reader modules, like their technologies, could make people track and RFID services their knowledge.

[Empire Readers](#)  
[RFID Reader Modules](#)  
[RFID Services](#)  
[www.thingmagic.com](http://www.thingmagic.com)

He filmed his heist, and soon his video intensified a debate over a push by some states, to put tracking technologies on their potential to erode privacy.

[See what GPS Tracking Web Downloaders Hide Beneath of GPS Tracking For Drivers \(Demo\)](#)  
[NavtrakGPS.com/GPS\\_Tracking\\_](http://NavtrakGPS.com/GPS_Tracking_)

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.

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.



(AP) In this April 10, 2009, photo, Chris Paget, a self-described "ethical" hacker, sits with his... [Full Image](#)

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

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.



(AP) In this April 9, 2009 photo, electronic readers and displays for NEXUS identification cards are...  
[Full Image](#)

Critics warn that RFID-tagged identities will enable identity thieves 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.

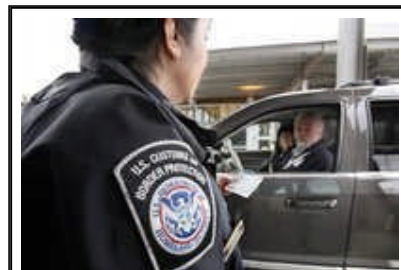
In a 2007 article published by a newsletter for privacy professionals, Pattinson called the chipped cards vulnerable "to attacks from hackers, identity thieves and possibly even terrorists."

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 issued caveats. 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."



(AP) In this April 9, 2009 photo, U.S. Customs and Border Protection officer Victoria Stephens speaks...  
[Full Image](#)

For now, chipped PASS cards and enhanced driver's licenses are 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.

But Gigi Zenk, a spokeswoman for the Washington state Department of Licensing, says Americans "aren't that concerned about the RFID" in a time when "tracking an individual is much easier through a cell phone."



In the wake of the Sept. 11 attacks - and the finding that some 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.



(AP) In this April 9, 2009 photo, a driver holds up a NEXUS identification card at a border crossing...

[Full Image](#)

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 and "fears that the U.S. Government or other governments would use the chip to track and censor, intimidate or otherwise control or harm them" were of "grave concern," it noted. Many Americans worried "that the information could be read at distances in excess of 10 feet."

Those 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 ... "

In 2005, the department incorporated metallic fibers into the e-passport's front cover, to reduce the read range, and added encryptions and a feature that required inspectors to optically scan the e-passport first for the chip to communicate wirelessly.

But what of 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 would emit radio waves only within a 4-inch radius, making it tougher to hack.

But in May 2006, at the University of Tel Aviv, researchers directly skimmed an encrypted tag from several feet away. At the University of Cambridge in Britain, a student intercepted a transmission between an e-passport and a legitimate reader 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)," Frank Moss, deputy assistant Secretary of State for passport services, 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.

In February 2006, an encrypted Dutch e-passport was hacked on national television, and later, British e-passports were hacked. The State Department countered that European e-passports weren't as safe as their American counterparts because they lacked safety features such as the anti-skimming cover. Recent studies have shown, however, that more powerful readers can



(AP) In this May 28, 2009 photo, a new "enhanced" United States passport lies, at left, beside an...

[Full Image](#)

penetrate that metal sheathing.

The RFIDs in enhanced driver's licenses and PASS cards contain 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, are intended to release their data to any inquiring Gen 2 reader within a 30-foot radius.

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

Still, computer experts 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 skimming RFID tags to track their targets, and fear government agents compiling 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.

Should biometrics 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.

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

Google sponsored links

[Intel® is the Future](#) - We're Involved In Science So Big You Can't See It. Get Involved Now!  
[www.Intel.com](http://www.Intel.com)

[Rfid Smart Card](#) - Find Rfid Smart Card. Search In Your Local Area Now.  
[OneClickLocal.com](http://OneClickLocal.com)

[New Spark Nano™ Device](#) - Smallest GPS Tracker In The World! Covert, Easy To Use, & Affordable  
[BrickHouseSecurity.com/NanoGPS](http://BrickHouseSecurity.com/NanoGPS)

## other high tech news

- [Computerized playground to open in Utah city](#)
- [Use caution at work on Internet, cell phone](#)
- [Young workers push employers for wider Web access](#)
- Chips in official IDs raise privacy fears
- [S. Korea analyzes computers used in cyberattacks](#)
- [Special alloy sleeves urged to block hackers?](#)
- [Social networking aggregator sues Facebook](#)
- [Smthg gr8 4 brkfst? Twitter's hyper-short recipes](#)
- [General Motors to try selling new cars on eBay](#)

- [AP proposes new article formatting for the Web](#)

 [email this page to a friend](#)

Copyright 2008 Associated Press. All right reserved. This material may not be published, broadcast, rewritten, or redistributed.



[Make My Way Your Home Page](#) | [Spread the Word](#) | [We're Hiring](#)

My Settings: [Overview](#) | [Search](#) | [Email](#) | [Chat](#) | [Portfolio](#) | [Calendar](#) | [Groups](#) | [Profile](#)

IMPORTANT: We do not present our users with pop-ups or any other non-contextual advertising. Nor do we send email to our users. If you see or receive one of these items, it is coming from an outside source, either as a result of something you have previously downloaded or as an "exit" pop-up from the site you just visited. It is not coming from our site.

[Privacy Policy](#) | [Terms of Service](#) | [About Us](#) | [Our Mission](#) | [Sign In](#) | [Sign Out](#) | [Help Center](#)

© 2008 IAC Search & Media. All rights reserved.

Partner Sites: [Citysearch](#) | [MerchantCircle](#) | [Insiderpages](#) | [CollegeHumor](#) | [Pronto](#) | [LiveDaily](#) | [Expedia](#) | [Hotels](#) | [Hotwire](#)  
[Evite](#) | [Excite](#) | [Fun Web Products](#) | [iWon](#) | [Smiley Central](#) | [Life123](#)