San Jose Mercury News

June 25, 2007

State needs law to protect personal data on chips

THE OPINION OF THE MERCURY NEWS EDITORIAL BOARD

Slap a chip costing a few cents on a clock radio or a bottle of Prozac, and you can track it from its manufacturer to the cash register at Wal-Mart. Build a chip into a special windshield tag, and it allows drivers to zip across the Golden Gate Bridge without stopping at a toll booth. Put one in a corporate identification card and all of a sudden it becomes an electronic door key.

Such is the power of radio frequency identification, or RFID, a technology that's been around for a half-century but is finally beginning to transform commerce — and become controversial.

It's just sinking in that the technology for tracking products can just as easily track people, and government agencies already have started using it. Before a major security breach occurs, the government must set some security and privacy standards for RFID chips that contain personal information.

And if the technology industry wants to boost public confidence in RFID, it should stop fighting reasonable regulation and help to craft solid data-protection rules.

RFID in its most basic form is totally unsecured. Anyone with a couple of hundred bucks and a little tech savvy can snoop on the data or even clone the chip without anyone's knowledge or consent.

That's not a problem when the chip is sending out harmless data like "this is a bag of potato chips." But it's different when the RFID tag contains personal information, such as a person's name, date of birth or Social Security number.

The U.S. government is already venturing into risky territory by embedding RFID chips in passports. This allows easy scanning of information, but it also could reveal personal data on U.S. citizens to unfriendly eyes.

California has an opportunity to set some standards before the technology is widely used by state and local governments. A sound policy could dissuade some of the craziest ideas. Remember the Sutter elementary school that issued RFID lanyards to kids a couple of years ago to track them throughout the day?

SB 30, sponsored by Sen. Joe Simitian, D-Palo Alto, lays out basic requirements for all government-issued identification documents in the state. The bill has passed the Senate, and the Assembly should send it to the governor.

Tech lobbying groups like AeA argue that regulation is unnecessary because abuses haven't yet occurred. It's a ludicrous position. The technology is just beginning to be used to identify individuals, and the potential for problems is so obvious. But the industry successfully lobbied Gov. Arnold Schwarzenegger to veto a similar bill last year.

Simitian's approach could use some tweaking. He has five separate bills on various aspects of RFID, from human implantation to criminal use of scanning devices, that really should be pared and consolidated. But Simitian's heart is in the right place.

Schwarzenegger voiced his own concern for identity protection when he first ran in the 2003 recall election and championed tougher security requirements for driver's licenses.

He needs to reaffirm his commitment to identity protection by making sure that government documents equipped with RFID chips are as safe and secure as possible.

The San Diego Union-Tribune

August 19, 2007

State bills aim to put controls on ID chip use

Growing technology has privacy groups worried

By Michael Gardner
COPLEY NEWS SERVICE

SACRAMENTO — With little thought, many Californians carry wafer-thin cards containing a 15-cent silicon chip that enable them to zip through toll booths, enter parking garages and access the office.

Called radio frequency identification, RFID technology is touted for its convenience and, more importantly, its security value at buildings, airports and borders.

But some say it comes at a price. Privacy rights advocates see a chilling side, warning that advances could offer new opportunities for identity thieves, furnish clues to stalkers and hand government another tool to spy on law-abiding citizens.

"Both sides are overplaying their hand," said Jim Harper, who monitors the issue for the Cato Institute, a libertarian think tank.

"The industry is trying to sell RFID as the hammer and every problem is the nail," he said. "The other side sees that and reacts with talk of banning RFID."

The chip is found in wallet-sized cards and tags attached to products for inventory control. A tiny wireless antenna transmits information, usually just an identifying number, to special

SEE **Security chip, A4**

AT ISSUE: RADIO FREQUENCY IDENTIFICATION

Across the country, debate rages over the merits and risks of this scanning technology. In California, lawmakers are considering limiting its use in government-issued cards.

Pros: Provides a better layer of security at airports and borders. Aids consumers by, for example, allowing motorists to zip through toll plazas. Improves inventory tracking for business.

Cons: Threatens privacy rights and can be exploited to steal identities and stalk victims. Gives government another instrument to monitor citizens.

▶ **SECURITY CHIP** CONTINUED FROM PAGE A1

Data can be lifted from a few feet away with a scanner, critics say

readers. The technology can be used to authorize access, subtract payments, track sales or confirm the identity of a passenger preparing to board a plane.

The federal Department of Homeland Security, in a push to better verify identities, has mulled requiring RFIDs in driver's licenses but has ruled it out for now.

Clashes over the growing reach of RFID into everyday life have escalated across the country. Groups that typically are adversaries, such as the Gun Owners of California and the American Civil Liberties Union, urge legal constraints. Powerful forces, such as bankers and retailers, have lined up against restrictions.

In California, lawmakers in the coming weeks are expected to act on legislation seeking to restrict the government's use of the technology. If successful, they would be the first laws of their kind in the nation, said

state Sen. Joe Simitian, a Palo Alto Democrat carrying five RFID-related measures.

"RFID has a million good uses. Tracking cattle, tracking soup is fine," Simitian said. "When you want to track California citizens, that's where it goes wrong."

His legislation would require the state, schools and other public agencies to impose special security measures before using the chip in items such as driver's licenses, health cards and school identification. The cards should be encrypted and armed with codes that only authorized readers can pick up, Simitian said.

The precautions can be met technologically but the cost of RFID will likely increase, various officials say.

Using these smart cards in the consumer product supply chain is relatively noncontroversial. But many people cringe at the idea of government and business knowing even more about individuals.

"The loudest debate is around privacy and security," said Michael Liard, a researcher who specializes in the technology for Boston-based ABI.

The RFID industry, now approaching $4 billion a year in sales, is expected to grow at a 20 percent annual clip, Liard said.

Backers of the technology note that security features are readily available to keep snooping and stealing to a minimum. They also stress its practical uses and convenience. For example, new credit cards use the technology to register inexpensive transactions without requiring a signature.

"Think bar codes that can talk," industry literature says.

Critics say that description is too simplistic. The technology has the potential to collect and store much more information than bar codes. This could expose the public to danger, infringe on privacy, and signal a retreat from the basic liberty to come and go as we please, they say. *Scientific American* magazine branded the use "human inventory control."

"If people buy into it without thinking, we've lost something very important in the American psyche," said Michael Ostrolenk, national director of the Liberty Coalition, an umbrella for civil liberties advocacy groups from People for the American Way to the Rutherford Institute.

"We have an ingrained dislike for the police state — the Soviet Union 'show me your papers' state," Ostrolenk said.

Industry officials say critics exaggerate the threat and understate the value of RFID.

"They make decisions based on not having the facts on what the technology can and cannot do," said Wolf Bielas, chief executive officer of RSI ID Technologies based in Chula Vista.

Joerg Borchert, a vice president of Infineon Technologies, said legislators are aiming at the wrong target. Instead, penalties for illegal use of stolen information should be more severe, he said.

"We should ban bad behavior — not the technology," Borchert said.

A crackdown could scare away investment and stifle innovation, Bielas and Borchert said.

"Technology is constantly evolving. Stopping technology or excluding certain technology can be counterproductive," Borchert said.

Asked Bielas: "When you kill it, what are you killing?"

Among the possibilities: Under-the-skin chips that can inform emergency medics of allergic reactions or other health problems even when the patient is unconscious. Refrigerators that could be programmed to read labels to ensure that milk, eggs and meat are still fresh.

"There's a lot of innovation left," said Alan Melling, Motorola's product management director.

That's exactly what has some so worried.

"We're talking about a technology that will only get smarter, smaller and cheaper for those who want to steal our information," Simitian said.

Critics say RFID data can be obtained by lifting the identifying number literally out of someone's pocket with a remote scanner from a couple of feet away. Databases could be accessed to match the number with other personal information. In one experiment, access cards of several legislative employees were remotely read in elevators and in hallways and cloned, providing the "thief" with access to private, secured areas.

"It sounds like science fiction, but it's quite doable," said Lee Tien, an attorney with the Electronic Frontier Foundation, an advocate for privacy rights in the digital world. "It's not paranoia if the threat is real."

Bielas disputed the ease of high-tech thievery, saying most cards cannot be read from much of a distance. "You have a better chance to read my credit card with very good eyes," he said.

Borchert pointed out that RFID cards and tags and the necessary databases can be shielded from prying. It would take powerful, expensive readers and familiarity with special databases to have even a remote opportunity to obtain private information, he said.

Examples are rare, but there are cases of theft and human tracking. Spanish police suspect thieves used RFID readers to lift the keyless access code and steal soccer star David Beckham's luxury BMW. Toll-road information has been subpoenaed in divorce cases to document someone's movements. A small country school near Sacramento monitored elementary students without parental approval until a mother blew the whistle.

"A young girl is an easy mark for predators," said Michele Tatro, whose daughter came home one day wearing a school-mandated identification tag. "They were trying to force us to have an electronic beacon." School administrators later backpedaled. But Tatro, fearing that using RFID in school identification cards could expose children to harm, continues to press her case in support of restraining its use in government-issued documents.

Another argument is offered by Mary Wiberg, executive director of the California Commission on the Status of Women, a state agency. A tech-savvy stalker could track habits of an intended victim by lifting data used to pass toll booths, park and enter buildings, she said.

"Thousands of women and children are the victims of crimes ... RFID technology would make illegal surveillance easier," Wiberg said.

Gov. Arnold Schwarzenegger has sided with industry in the past but is noncommittal toward Simitian's measures.

The Republican governor vetoed a bill limiting RFID last year, calling it "premature" and voicing concern that the measure could "unduly burden the numerous new applications" of the technology.

Simitian calls his goals for tighter security "common sense."

"Why do we have locks on our doors? Because we have something of value inside," he said.

> "RFID has a million good uses. Tracking cattle, tracking soup is fine. When you want to track California citizens, that's where it goes wrong."
>
> **JOE SIMITIAN**
> *Democratic state senator from Palo Alto*

PROPOSED LEGISLATION

State Sen. Joe Simitian, a Palo Alto Democrat, is carrying five measures to restrict scanning technology.

SB 28: Prohibits the state from embedding identifying chips in driver's licenses.

SB 29: Bars K-12 schools from using radio frequency identification technology in identification cards.

SB 30: Requires special security for all state-issued identification, such as driver's licenses and health care cards. Safeguards would include encryption and shields. Recipients would be notified about the RFID technology.

SB 31: Makes it illegal to surreptitiously read or record information from an identification card. Bars the disclosure of codes that enable scanners to pick up information from cards.

SB 362: Prohibits companies and the government from compelling employees to accept under-the-skin implantation of identifying chips.

For more information: Go to www.senate.ca.gov. Click on "legislation" and enter the individual bill number.

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

October 2, 2008

California Bans RFID Skimming

Advocates of the bill say it will help maintain security for millions of state residents who use the technology in their everyday lives.

By K.C. Jones

It's now illegal to surreptitiously read RFID tags in California.

The state's governor, Arnold Schwarzenegger, signed SB 31 into law Tuesday. The legislation makes it "illegal to take information from RFID tags" without an owner's knowledge and permission. Exemptions allow emergency medical workers and law enforcement to scan RFID tags to identify unresponsive people or solve crimes, as long as they have obtained a warrant.

"The problem is real," said State Sen. Joe Simitian, a Palo Alto Democrat who introduced the legislation. "Millions of Californians use RFID cards to gain access to their office, apartment, condo, day care center or parking garage. Our passports now use the technology, and there is continued discussion about the possible use of RFID in drivers' licenses. Yet, up till now, there's been no law on the books to prevent anyone from skimming your information, and it's surprisingly easy to do." Simitian conducted an experiment in which his access card for the State Capitol was skimmed and cloned by a hacker in a second.

"Minutes later, using that clone of my card, the hacker was able to walk right into the Capitol through a 'secure' and locked entrance," he said. "RFID technology is not in and of itself the issue. RFID is a minor miracle with all sorts of good uses, but it's easier than ever to steal someone's personal information. With an unauthorized reader – technology that is readily available, off-the-shelf, and surprisingly inexpensive it's really quite simple to do." Simitian said the public would resist emerging technologies without privacy and security protections.

The new law drew support from a wide variety of groups, including: the American Civil Liberties Union, Gun Owners of California. Privacy Rights Clearinghouse, Citizens Against Government Waste, California State Parent Teacher Association (PTA), Republican Liberty Caucus, and the National Organization for Women (NOW). Nicole Ozer, technology and civil liberties policy director for the ACLU of Northern California, praised Schwarzenegger for signing the bill into law.

"Just like Californians wouldn't allow a stranger to sift through their wallet and take their driver's license or want their children or grandchildren to tell passers-by on the street who they are or where they live, our private information must not be read at a distance without our knowledge or consent," she said. "By signing SB 31, Governor Schwarzenegger has taken an important step to safeguard the privacy, personal and public safety, and financial security of millions of families."