California could become third state to ban forced microchip tag implants (RFID)

By Orr Shtuhl
Global Research, January 12, 2008
Stateline.org 18 September 2007

Region: USA
Theme: Police State & Civil Rights

Photo courtesy of VeriChip Corp.
The VeriChip implantable RFID tag, made up of a microchip and an antenna encased in glass, is 12 mm long and 2 mm in diameter, about the size of a grain of rice.

It would be an interesting feature of an employee's first day: sign a contract, fill out a W-2 and roll up your sleeve for your microchip injection.

Sounds like sci-fi, but it's happened, and now a handful of states are making sure their citizens will never be forced to have a microchip implanted under their skin.

If Gov. Arnold Schwarzenegger (R) signs a bill passed Sept. 4, California would join Wisconsin and North Dakota in banning human implanting of these tags without consent.

No one's quite sure how real a threat these forced implants might be, or why states are feeling compelled to protect their residents from being physically tagged. Lawmakers are calling the legislation pre-emptive, while the industry that produces the technology sees the states' action as fear mongering.

Radio-frequency identification (RFID) tags – tiny, data-storing microchips about the size of a grain of rice – are in passports, in Wal-Mart factory shipments and in subway passes in cities from New York to Taiwan. They are also in humans. On one less-than-likely episode of "Law & Order: Special Victims Unit," a paranoid actor Bob Saget even uses one to monitor his adulterous wife.

Unlike Global Positioning System (GPS) technology, which is used for constant, real-time tracking, RFID tags are scanned at close range – usually from a few feet to a few inches. The tags are tracked by scanners installed at checkpoints, such as office doors or warehouse loading docks. The systems are also commonly used in highway toll collection and as theft protection in car keys.

In humans, they have been used to store medical information, to track movement and to gain access to locked rooms. To date, 2,000 RFID chips have been sold for implantation in humans, says VeriChip Corp., the only manufacturer with a Food and Drug Administration-approved implantable chip.

The company is focusing its technology on medical patient identification, and about 400

patients, including those with Alzheimer's disease, have RFIDs implanted. Other VeriChip human implants have been used by a Spanish nightclub to allow VIPs with implanted chips to bypass entrance lines and by the Mexico attorney general's staff to safeguard identity information at a time when the kidnapping of government officials there is not uncommon.

Some customers are using them as high-tech keys. Ohio security firm CityWatcher.com raised eyebrows in 2006 when it requested that some of its employees be "chipped," or implanted with tags for access to certain rooms. According to published reports, only two employees got the implants before the company dropped the program. CityWatcher.com has since shut down.

But forced chipping has been a rare practice, leading some industry spokespeople to decry regulation as "scare tactics."

Wisconsin enacted the first RFID ban in May 2006, and North Dakota in April. Colorado and Ohio have bills in committee, and Oklahoma and Florida saw theirs die last session. Except for one U.S. House proposal to use RFID tags to track prescription drugs, Congress has not widely addressed the technology.

Legislators admit that the few laws being enacted are pre-emptive. Wisconsin state Rep. Marlin Schneider (D) had never heard of CityWatcher.com when he drafted the first implant ban.

"I had heard about this device from CNN or someplace, and I went into the office and said, 'Get a bill drafted that prohibits this,'" he said. "This is beyond even what Orwell imagined."

State Sen. Joe Simitian (D), who authored California's bill, said he first looked into RFID legislation after grade schools in Sutter County, Calif., required students to wear IDs containing the chips to help monitor attendance. The move prompted privacy complaints from parents, and the school eventually stopped using the technology.

Simitian introduced four other RFID bills, dealing with criminal punishment for identity theft, security standards and use of these tags in driver's licenses and school IDs.

All four proposals were originally pieces of California's Identity Information Protection Act of 2006, which passed but was vetoed by Schwarzenegger. In a statement, he recommended waiting for standards from the federal Real ID Act, a plan to organize states' driver's licenses into a national system. The governor has until Oct. 14 to sign or veto the newly passed bill.

The lack of security in the chips is particularly alarming, Simitian said, and is a major reason he thinks the state should step in with regulation. A May 2006 story in *Wired Magazine* featured Jonathan Westhues, a 24-year-old engineer who demonstrated how he could (and did) covertly scan a company's RFID employee badge and break into the office – all with a cheap, homemade reader. He's since posted detailed instructions on how to make the reader on his Web site.

Westhues likens RFID chips to "a repurposed dog tag. … The Verichip is built with no attempt at security, and is therefore not very special to clone," he writes on his Web site.

How low-tech are these homemade readers?

Determined to show the security flaws to skeptics in the Legislature, Simitian asked a tech-savvy grad student from his office to build one. The student then wandered the state Capitol one afternoon with the reader in his briefcase. In the process, he stole the security numbers of nine representatives. The reader could send out any of those numbers, getting him past any locked door a state senator would have access to. And he would appear as the senator in the electronic records.

Manufacturers and industry representatives say that no cases of such identity theft have been documented. But depending on the desired level of security, cameras and guards should be used in addition to RFID tags, says the AeA (formerly the American Electronics Association).

The technology is being embraced by a few government agencies. Both Vermont and Washington state have agreed to work with the Department of Homeland Security to test RFID driver's licenses, although they won't be required by citizens. The U.S. Department of Defense has been tracking shipments with RFID tags since 2003.

Besides possible privacy breaches, the new technology also has raised health alarms. Studies of implants used in the past 12 years have linked RFIDs to cancer in lab mice and rats, according to The Associated Press.

The studies did not have control groups for the cancer, and manufacturers report no complications with the millions of pets that have had various chip implants over the last 15 years. But the results were enough for some scientists to question the FDA's approval of the technology.

Comment on this story in the space below by registering with Stateline.org, or e-mail your feedback to our Letters to the editor sectionat letters@stateline.org.

Contact Orr Shtuhl at editor@stateline.org.

Related stories:

California law on ID theft seen as model
Real ID dropouts leave security holes
States' rebellion at Real ID echoes in Congress
Two states lead revolt against Real ID
Real ID deadline delayed
Are you a citizen? Prove it

Articles by: Orr Shtuhl