

Chips: High Tech Aids or Tracking Tools?

By TODD LEWAN, AP National Writer
July 22, 2007

CityWatcher.com, a provider of surveillance equipment, attracted little notice itself - until a year ago, when two of its employees had glass-encapsulated microchips with miniature antennas embedded in their forearms.

The "chipping" of two workers with RFIDs - radio frequency identification tags as long as two grains of rice, as thick as a toothpick - was merely a way of restricting access to vaults that held sensitive data and images for police departments, a layer of security beyond key cards and clearance codes, the company said.



"To protect high-end secure data, you use more sophisticated techniques," Sean Darks, chief executive of the Cincinnati-based company, said. He compared chip implants to retina scans or fingerprinting. "There's a reader outside the door; you walk up to the reader, put your arm under it, and it opens the door."

Innocuous? Maybe.

But the news that Americans had, for the first time, been injected with electronic identifiers to perform their jobs fired up a debate over the proliferation of ever-more-precise tracking technologies and their ability to erode privacy in the digital age.

To some, the microchip was a wondrous invention - a high-tech helper that could increase security at nuclear plants and military bases, help authorities identify wandering Alzheimer's patients, allow consumers to buy their groceries, literally, with the wave of a chipped hand.

To others, the notion of tagging people was Orwellian, a departure from centuries of history and tradition in which people had the right to go and do as they pleased, without being tracked, unless they were harming someone else.

Chipping, these critics said, might start with Alzheimer's patients or Army Rangers, but would eventually be suggested for convicts, then parolees, then sex offenders, then illegal aliens - until one day, a majority of Americans, falling into one category or another, would find themselves electronically tagged.

The concept of making all things traceable isn't alien to Americans. Thirty years ago, the first electronic tags were fixed to the ears of cattle, to permit ranchers to track a herd's

reproductive and eating habits. In the 1990s, millions of chips were implanted in livestock, fish, dogs, cats, even racehorses.

Microchips are now fixed to car windshields as toll-paying devices, on "contactless" payment cards (Chase's "Blink," or MasterCard's "PayPass"). They're embedded in Michelin tires, library books, passports, work uniforms, luggage, and, unbeknownst to many consumers, on a host of individual items, from Hewlett Packard printers to Sanyo TVs, at Wal-Mart and Best Buy.

But CityWatcher.com employees weren't appliances or pets: They were people made scannable.

"It was scary that a government contractor that specialized in putting surveillance cameras on city streets was the first to incorporate this technology in the workplace," says Liz McIntyre, co-author of "Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID."

Darks, the CityWatcher.com executive, dismissed his critics, noting that he and his employees had volunteered to be chip-injected. Any suggestion that a sinister, Big-Brother-like campaign was afoot, he said, was hogwash.

"You would think that we were going around putting chips in people by force," he told a reporter, "and that's not the case at all."

Yet, within days of the company's announcement, civil libertarians and Christian conservatives joined to excoriate the microchip's implantation in people.

RFID, they warned, would soon enable the government to "frisk" citizens electronically - an invisible, undetectable search performed by readers posted at "hotspots" along roadsides and in pedestrian areas. It might even be used to squeal on employees while they worked; time spent at the water cooler, in the bathroom, in a designated smoking area could one day be broadcast, recorded and compiled in off-limits, company databases.

"Ultimately," says Katherine Albrecht, a privacy advocate who specializes in consumer education and RFID technology, "the fear is that the government or your employer might someday say, 'Take a chip or starve.'"

Some Christian critics saw the implants as the fulfillment of a biblical prophecy that describes an age of evil in which humans are forced to take the "Mark of the Beast" on their bodies, to buy or sell anything.

Gary Wohlscheid, president of These Last Days Ministries, a Roman Catholic group in Lowell, Mich., put together a Web site that linked the implantable microchips to the apocalyptic prophecy in the book of Revelation.

"The Bible tells us that God's wrath will come to those who take the Mark of the Beast," he says. Those who refuse to accept the Satanic chip "will be saved," Wohlscheid offers in a comforting tone.

In post-9/11 America, electronic surveillance comes in myriad forms: in a gas station's video camera; in a cell phone tucked inside a teen's back pocket; in a radio tag attached to a supermarket shopping cart; in a Porsche automobile equipped with a LoJack anti-theft device.

"We're really on the verge of creating a surveillance society in America, where every movement, every action - some would even claim, our very thoughts - will be tracked, monitored, recorded and correlated," says Barry Steinhardt, director of the Technology and Liberty Program at the American Civil Liberties Union in Washington, D.C. RFID, in Steinhardt's opinion, "could play a pivotal role in creating that surveillance society."

In design, the tag is simple: A medical-grade glass capsule holds a silicon computer chip, a copper antenna and a "capacitor" that transmits data stored on the chip when prompted by an electromagnetic reader.

Implantations are quick, relatively simple procedures. After a local anesthetic is administered, a large-gauge hypodermic needle injects the chip under the skin on the back of the arm, midway between the elbow and the shoulder.

"It feels just like getting a vaccine - a bit of pressure, no specific pain," says John Halamka, an emergency physician at Beth Israel Deaconess Medical Center in Boston.

He got chipped two years ago, "so that if I was ever in an accident, and arrived unconscious or incoherent at an emergency ward, doctors could identify me and access my medical history quickly." (A chipped person's medical profile can be continuously updated, since the information is stored on a database accessed via the Internet.)

Halamka thinks of his microchip as another technology with practical value, like his BlackBerry. But it's also clear, he says, that there are consequences to having an implanted identifier.

"My friends have commented to me that I'm 'marked' for life, that I've lost my anonymity. And to be honest, I think they're right."

Indeed, as microchip proponents and detractors readily agree, Americans' mistrust of microchips and technologies like RFID runs deep. Many wonder: do the current chips have global positioning transceivers that would allow the government to pinpoint a person's exact location, 24-7? (No; the technology doesn't yet exist.)

But could a tech-savvy stalker rig scanners to video cameras and film somebody each time they entered or left the house? (Quite easily, though not cheaply. Currently, readers cost \$300 and up.)

How about thieves? Could they make their own readers, aim them at unsuspecting individuals, and surreptitiously pluck people's IDs out of their arms? (Yes. There's even a name for it - "spoofing.")

What's the average lifespan of a microchip? (About 10-15 years.) What if you get tired of it before then - can it be easily, painlessly removed? (Short answer: No.)

Presently, Steinhardt and other privacy advocates view the tagging of identity documents - passports, drivers licenses and the like - as a more pressing threat to Americans' privacy than the chipping of people. Equipping hospitals, doctors' offices, police stations and government agencies with readers will be costly, training staff will take time, and, he says, "people are going to be too squeamish about having an RFID chip inserted into their arms, or wherever."

But that wasn't the case in March 2004, when the Baja Beach Club in Barcelona, Spain - a nightclub catering to the body-aware, under-25 crowd - began holding "Implant Nights."

In a white lab coat, with hypodermic in latex-gloved hand, a company chipper wandered through the throng of the clubbers and clubbets, anesthetizing the arms of consenting party goers, then injecting them with microchips.

The payoff? Injectees would thereafter be able to breeze past bouncers and entrance lines, magically open doors to VIP lounges, and pay for drinks without cash or credit cards. The ID number on the VIP chip was linked to the user's financial accounts and stored in the club's computers.

After being chipped himself, club owner Conrad K. Chase declared that chip implants were hardly a big deal to his patrons, since "almost everybody has piercings, tattoos or silicone."

VIP chipping soon spread to the Baja Beach Club in Rotterdam, Holland, the Bar Soba in Edinburgh, Scotland, and the Amika nightclub in Miami Beach, Fla.

That same year, Mexico's attorney general, Rafael Macedo, made an announcement that thrilled chip proponents and chilled privacy advocates: He and 18 members of his staff had been microchipped as a way to limit access to a sensitive records room, whose door unlocked when a "portal reader" scanned the chips. But did this make Mexican security airtight?

Hardly, says Jonathan Westhues, an independent security researcher in Cambridge, Mass. He concocted an "emulator," a hand-held device that cloned the implantable microchip electronically. With a team of computer-security experts, he demonstrated - on television - how easy it was to snag data off a chip.

Explains Adam Stubblefield, a Johns Hopkins researcher who joined the team: "You pass within a foot of a chipped person, copy the chip's code, then with a push of the button, replay the same ID number to any reader. You essentially assume the person's identity."

The company that makes implantable microchips for humans, VeriChip Corp., of Delray Beach, Fla., concedes the point - even as it markets its radio tag and its portal scanner as imperatives for high-security buildings, such as nuclear power plants.

"To grab information from radio frequency products with a scanning device is not hard to do," Scott Silverman, the company's chief executive, says. However, "the chip itself only contains a unique, 16-digit identification number. The relevant information is stored on a database."

Even so, he insists, it's harder to clone a VeriChip than it would be to steal someone's key card and use it to enter secure areas.

VeriChip Corp., whose parent company has been selling radio tags for animals for more than a decade, has sold 7,000 microchips worldwide, of which about 2,000 have been implanted in humans. More than one-tenth of those have been in the U.S., generating "nominal revenues," the company acknowledged in a Securities and Exchange Commission filing in February.

Although in five years VeriChip Corp. has yet to turn a profit, it has been investing heavily - up to \$2 million a quarter - to create new markets.

The company's present push: tagging of "high-risk" patients - diabetics and people with heart conditions or Alzheimer's disease. In an emergency, hospital staff could wave a reader over a patient's arm, get an ID number, and then, via the Internet, enter a company database and pull up the person's identity and medical history.

To doctors, a "starter kit" - complete with 10 hypodermic syringes, 10 VeriChips and a reader - costs \$1,400. To patients, a microchip implant means a \$200, out-of-pocket expense to their physician. Presently, chip implants aren't covered by insurance companies, Medicare or Medicaid.

For almost two years, the company has been offering hospitals free scanners, but acceptance has been limited. According to the company's most recent SEC quarterly filing, 515 hospitals have pledged to take part in the VeriMed network, yet only 100 have actually been equipped and trained to use the system.

Some wonder why they should abandon noninvasive tags such as MedicAlert, a low-tech bracelet that warns paramedics if patients have serious allergies or a chronic medical condition. "Having these things under your skin instead of in your back pocket - it's just not clear to me why it's worth the inconvenience," says Westhues.

Silverman responds that an implanted chip is "guaranteed to be with you. It's not a medical arm bracelet that you can take off if you don't like the way it looks..."

In fact, microchips can be removed from the body - but it's not like removing a splinter.

The capsules can migrate around the body or bury themselves deep in the arm. When that happens, a sensor X-ray and monitors are needed to locate the chip, and a plastic surgeon must cut away scar tissue that forms around the chip.

The relative permanence is a big reason why Marc Rotenberg, of the Electronic Privacy Information Center, is suspicious about the motives of the company, which charges an annual fee to keep clients' records.

The company charges \$20 a year for customers to keep a "one-pager" on its database - a record of blood type, allergies, medications, driver's license data and living-will directives. For \$80 a year, it will keep an individual's full medical history.

In recent times, there have been rumors on Wall Street, and elsewhere, of the potential uses for RFID in humans: the chipping of U.S. soldiers, of inmates, or of migrant workers, to name a few. To date, none of this has happened.

But a large-scale chipping plan that was proposed illustrates the stakes, pro and con. In mid-May, a protest outside the Alzheimer's Community Care Center in West Palm Beach, Fla., drew attention to a two-year study in which 200 Alzheimer's patients, along with their caregivers, were to receive chip implants. Parents, children and elderly people decried the plan, with signs and placards.

"Chipping People Is Wrong" and "People Are Not Pets," the signs read. And: "Stop VeriChip."

Ironically, the media attention sent VeriChip's stock soaring 27 percent in one day. "VeriChip offers technology that is absolutely bursting with potential," wrote blogger Gary E. Sattler, of the AOL site Bloggingstocks, even as he recognized privacy concerns.

Albrecht, the RFID critic who organized the demonstration, raises similar concerns on her AntiChips.com Web site.

"Is it appropriate to use the most vulnerable members of society for invasive medical research? Should the company be allowed to implant microchips into people whose mental impairments mean they cannot give fully informed consent?"

Mary Barnes, the care center's chief executive, counters that both the patients and their legal guardians must consent to the implants before receiving them. And the chips, she says, could be invaluable in identifying lost patients - for instance, if a hurricane strikes Florida.

That, of course, assumes that the Internet would be accessible in a killer storm. VeriChip Corp. acknowledged in an SEC filing that its "database may not function properly" in such circumstances.

As the polemic heats up, legislators are increasingly being drawn into the fray. Two states, Wisconsin and North Dakota, recently passed laws prohibiting the forced implantation of microchips in humans. Others - Ohio, Oklahoma, Colorado and Florida - are studying similar legislation.

In May, Oklahoma legislators were debating a bill that would have authorized microchip implants in people imprisoned for violent crimes. Many felt it would be a good way to monitor felons once released from prison.

But other lawmakers raised concerns. Rep. John Wright worried, "Apparently, we're going to permanently put the mark on these people."

Rep. Ed Cannaday found the forced microchipping of inmates "invasive ... We are going down that slippery slope."

In the end, lawmakers sent the bill back to committee for more work.