Article from SIRS Discoverer Database; (ProQuest) Lexile:1230L

Identity Chips Could Protect Health, but Hurt Privacy, Some Say

CHICAGO TRIBUNE
(Chicago, IL)
Dec. 24, 2004, n.p.

Identity Chips Could Protect Health, but Hurt Privacy, Some Say

By Vincent J. Schodolski
Chicago Tribune

LOS ANGELES--As many as 2,000 people in the world are walking around with rice-sized chips under their skin that can allow others to find out a great deal of information about them.

Want to know if the individual has had his gall bladder removed or has a pacemaker? Want to make sure the person handing you a credit card really is who he says he is?

If you are the person's employer, do you want to know exactly where she is during the workday?

This may all sound like "1984" and raise alarms about **privacy**, but some experts are confident there are ways to prevent unwanted snooping in chip users' personal affairs. And they contend existing laws are sufficient to catch and punish anybody who tries.

In October, the Food and Drug Administration approved the chip for **medical** use, a reason many of those with a chip cite for wanting it.

One intended use, for example, is to allow emergency room doctors access to the **medical** records of someone unable to communicate.

"Say you live in L.A., but get hit by a car in New York," said Scott Silverman, chairman and chief executive officer of Applied Digital, the Delray Beach, Fla., manufacturer of VeriChip, an embedded device.

VeriChip is one of several devices that employ radio frequency identification, or RFID, technology to accomplish rapid and remote transmission of information.

Each VeriChip, the only RFID device actually implanted in a user's body, contains a 16-digit identification number than can be read by a person using a scanner that activates the chip and tells it to transmit the number.

In a phone interview, Silverman said each person with a VeriChip implant has designated certain individuals--typically family members--who are permitted to access user information.

Each VeriChip user carries a card explaining how to use the technology, Silverman said. And designated persons must submit their own ID numbers to Applied Digital before they can obtain the user data from a company database.

Silverman said he is confident the system is secure. He said even if someone stole one of the scanners, the thief would need a user ID to access the data.

In other uses, such as validating the identity of a credit-card user, the VeriChip technology makes identity theft more difficult, Silverman said.

"We think VeriChip can be used to enhance your **privacy**," he said.

Experts say the same chip that can identify you also can be activated by scanners to allow authorized people to open doors simply by approaching them. It is the equivalent of swiping an ID card across a reader next to the door.

Similarly, scanners can be positioned throughout a building to track people as they move about.

Some are skeptical of the technology used by Applied Digital.

"The VeriChip is neither as good as its marketing nor as bad as its critics suggest," said Jean Camp, an associate professor of informatics--the study of how data are processed and transmitted--at Indiana University in Bloomington.

"The VeriChip gives each implanted individual a number that, in turn, links to a database of information," Camp, who studies **privacy** issues, said in an e-mail exchange. "Like a biometric"--a physical identifier, such as a fingerprint or iris pattern--"it is a data element that cannot be changed and that you cannot forget. Like a biometric, you go around sharing that data just by existing.

"The **privacy** problems in this system are the security problems. The security problem is that you have one number, that number provides access to all your personal information and you walk around broadcasting that number."

She disagreed with Silverman, saying it would be easy to gain access to the chip ID number.

"If I wanted to steal your identity under this model it appears (all) I would have to do is get an RFID reader for a few hundred dollars. I could then read your VeriChip ID as you walk past.

"Then I would write an RFID with the same number, and implant it in my own arm. Voila! Identity theft made wireless."

Some believe that any new technology ultimately can be hacked or protected by newer technology.

"At this stage it does not seem to be much of a problem," said David MacDonald, an attorney who practices **privacy** law.

MacDonald, in a phone interview, suggested that in the case of any RFID device, an individual could vanish simply by wearing a transmitter with a stronger signal than the device in question.

He said potential uses of RFID devices could cause **privacy** concerns.

He suggested a politician might be able to make a case for embedding all children with chips to deter kidnapping. "It might even be a good idea," he said.

But the Orwellian aspects of that are plain. Once you have scanners all around the country to track children, the government would obtain mountains of private information.

He suggested that the use of a VeriChip to back up confirmation of a credit card's valid use was a good idea.

"Two factors are always more secure than one," he said. "The chip would be hard to replicate. You might not notice that someone took your credit card, but you would notice if someone took a chip embedded in your arm."

MacDonald also was confident that existing laws could protect users of RFID technology against fraud. If anyone got access to your data--just as if they stole a credit card--the unauthorized use of that information would be a crime.

"Generally, existing laws will protect because of the consent issue," he said.