

**A “VeriChip” on Society’s Shoulder:
Positive and Negative Implications of the VeriChip©**

Steve Lacznik
Department of Engineering Physics
University of Wisconsin-Madison

Table of Contents

Executive Summary	iii
Introduction	1
The VeriChip	2
What is the VeriChip?	2
How does a VeriChip System Work?	3
Positive Implications of the VeriChip	4
The Healthcare Sector	4
An Additional Layer of Security	5
Special Cases: e.g. Katrina	6
Negative Implications of the VeriChip	6
Will Privacy be Lost?	7
What about Health Risks?	8
How Secure is the VeriChip?	9
A “VeriChip” on Society’s Shoulder	10
Glossary	12
References	13

Executive Summary

On October 12, 2004, the Food and Drug Administration approved the VeriChip for medical use. The VeriChip (a tiny, human-implantable RFID tag) may offer some people safety and convenience; but, many others find the device unsettling. While the VeriChip can play an important—even life-saving—role in the healthcare sector, the sub-dermal RFID tag makes potential users more vulnerable to privacy loss.

In medicine, the VeriChip primarily functions as a tool for managing patient information. Specifically, the chip allows healthcare professionals to quickly and accurately ascertain critical patient information. The device, which contains only a unique serial number, is linked to a patient database maintained by a hospital. Typically, the database information would include a person's name, address, current medications, known allergies and critical medical history. Key constituents who would benefit from a VeriChip include anyone with impaired speech, memory loss or chronic loss of consciousness. These conditions create a communication barrier that could delay treatment or even result in medical errors. To remedy this situation, the VeriChip conveys pertinent information when the patient is unable to do so. In this manner, the VeriChip fills a possible information gap in the healthcare sector, and the device should be considered as a preventative tactic for at-risk individuals. Already, hospitals are accepting the technology. As of October 3, 2005, fifty-eight hospitals across the United States have agreed to implement a patient identification VeriChip system in their emergency rooms.

Interlocking databases remain a concern with respect to VeriChip systems. Critics of the device contend that these VeriChip databases may become linked to other private and public databases. These interlocking databases make complete profiles on any consumer available. Such biographical sketches might include name, address, social security number, credit reports and—with the addition of VeriChip databases—even medical records. Companies, such as the data broker ChoicePoint, will start maintaining databases of RFID numbers and their associated parties. The problem is that these aggregate databases are a tempting target for criminals. Also, companies who gain access to the information could use it surreptitiously to make employment decisions. In February, ChoicePoint accidentally sold confidential information on 145,000 people to identity thieves posing as legitimate businessmen. Introducing the VeriChip creates the potential for a person's medical history to be included in these cumulative databases. In the end, consumers have little reassurance that VeriChip databases will remain private and separated from other databases and data brokers. Consumers considering the VeriChip should be weary as their personal information will be at the discretion of whoever controls the accompanying VeriChip database.

Introduction

In March 2004, a Barcelona nightclub started offering VeriChip services to its regular clients. Revelers with the implanted microchip could use the device to bypass entry lines and manage their bar tabs (See Figure 1). A few months later, on October 12, 2004, the Food and Drug Administration (FDA) approved the VeriChip for medical purposes. With medical use already approved in the United States and plans for security and financial applications underway, the VeriChip Corporation—the company that makes the VeriChip—is looking to grow its product in the coming years. While the VeriChip may offer some people safety and convenience, the device appears unsettling to others. For instance, John L. Peterson, a security expert and futurist at the Arlington Institute in Washington D.C., commented on the chipping of humans: “In a decade or two, there will be a commonly available system with the ability to know who people are, where they are and what they’ve done” (Murray, 2004, p. 1). Is the VeriChip a first step towards the “Big Brother” society that Peterson predicts? Or, is the VeriChip a device that can provide added convenience to consumers?



Figure 1. *The VeriChip in use.* A bouncer scans a club patron’s VeriChip at the Baja Beach Club in Barcelona. This reveler uses her VeriChip to gain quick entrance to the nightclub and manage her tab. Source: <http://www.erenouvelle.com/newpuce.php/>

This technical report will focus on the impact that a VeriChip system will have on society. In other words, this document will address the positive and negative implications of the VeriChip. Indeed, the VeriChip offers a number of beneficial uses for consumers.

In the ER: The device functions as a means of communicating critical healthcare information for patients who are incapable of speaking. For instance, a VeriChip tied to a medical database could be lifesaving for an unconscious patient in the emergency room. The emergency room technicians could scan the victim’s VeriChip and instantly receive information about the patient’s current medications, known allergies and primary caregiver (<http://www.verichipcorp.com/>).

At the ATM: Deploying a VeriChip system may increase a person’s financial security. Approximately fifty percent of all debit-card fraud occurs when a card is stolen by someone who knows the personal identification number of the victim (Sidel, 2005). With a VeriChip tied to a credit or debit card, card readers equipped with a VeriChip scanner would authorize transactions only if the matching VeriChip is in range. This means that

someone who knows a pin number—but does not have the correct VeriChip—could not use a snagged debit card (Scheeres, 2005).

Despite the huge upside of this emerging technology, there remains widespread criticism of the device. VeriChips have the negative potential of limiting a person's privacy. Given the increased incidence of *interlocking databases*^{*}, third parties could link a person's VeriChip with a myriad of other information such as the books that one purchased from Barnes & Noble or specific financial information that was revealed as part of a credit application (Schneier, 2005). Moreover, a person with a sub-dermal VeriChip could potentially have their movements and transactions monitored by an unauthorized, clandestine party. Certainly, such negative aspects will weigh heavily on a person's individual decision regarding whether or not to get "chipped".

The VeriChip

Engineered by Applied Digital Solutions Inc., the VeriChip—as the name implies—is a microprocessor used for verification and identification purposes. Implantable under human skin, the device can convey personally identifiable information such as one's medical history, credit-card number, security clearance and even club membership status. According to a September 2005 article in Red Herring, a business technology news magazine, approximately 50 people in the United States currently have VeriChip implants ("Banker gets ID Chip Implant," 2005). While this domestic number is low, hundreds of people are chipped worldwide (Murray, 2004). As the VeriChip Corporation ships more units to hospitals and businesses, the number of VeriChip implants will continue to grow. This fact holds substantial consequences for society. In order to understand the implications that the VeriChip may create for society, it is important to be familiar with how a VeriChip actually works as well as how an entire VeriChip system operates.

What is the VeriChip?

Simply put, the VeriChip is a *radiofrequency identification (RFID) tag*. Manufactured and marketed by VeriChip Corporation, the tiny microprocessor measures 12 mm long and 2.1 mm in diameter. The device is roughly the size of a grain of rice (See Figure 2). Typically, a doctor inserts the device behind the triceps of the right arm between the elbow and shoulder using a syringe. A proficient doctor may complete the procedure in less than 20 seconds, and the insertion currently costs about 200



Figure 2. *The VeriChip.* A VeriChip is roughly the size of a grain of rice.
Source: <http://www.verichipcorp.com/>

^{*} Italicized words are defined in the glossary, page 12.

dollars (Dishneau, 2005). Focusing again on technical details, the VeriChip incorporates two major components into its medical-grade glass container: a small microchip and an antenna. First, the microchip functions as the VeriChip's circuitry—it contains a radio receiver and modulator as well as control logic and storage memory. Second, a small piece of coiled wire functions as the antenna (Garfinkel, 2005). Interestingly, the VeriChip does not contain a battery. Instead, the chip derives the necessary electrical power to transmit its signal using the coiled antenna through a physical property known as *inductance*. Because the VeriChip does not contain a battery, it is considered a *passive RFID tag*. Essentially, this means that the microchip will remain inactive until it is activated by a proprietary scanner.

Passive RFID tags, like the VeriChip, boast a number of unique, significant features. For starters, passive RFID tags have longer lifetimes than *active RFID tags*—tags with onboard batteries. In fact, the estimated lifetime of a VeriChip is over 20 years. Next, passive RFID tags can only broadcast low-frequency radiowaves because of their minimal power. In the VeriChip's case, it broadcasts on the low-frequency (LF) band between 125 and 134.2 KHz (Fox, 2004). Given the VeriChip's low power, the tag is only able to communicate with devices inside a range of a few feet. Because of the VeriChip's limited transmission range, the device is suitable for identification applications. The VeriChip contains and transmits only a unique, 16-digit identification number—in this manner, the VeriChip can be thought of like a bar code. By itself, the VeriChip does not immediately reveal identifying information, but when tied to a database, it may provide significant information.

How does a VeriChip System Work?

VeriChip systems involve three components—the VeriChip, a scanner and a database. First, a proprietary scanner sends out an excitatory signal (See Figure 3). This signal is a radiowave capable of activating a dormant VeriChip. If the scanner is within range of a VeriChip, the chip will return a unique 16-digit identification number. The scanner then relays that ID number to a secure database via the Internet. After interpreting the identification number, the database returns the requested information to the scanner. The provided information may now be used as desired (<http://www.verichipcorp.com/>).

Here is a hypothetical example of the VeriChip in action. Imagine that a University of Wisconsin-Madison student

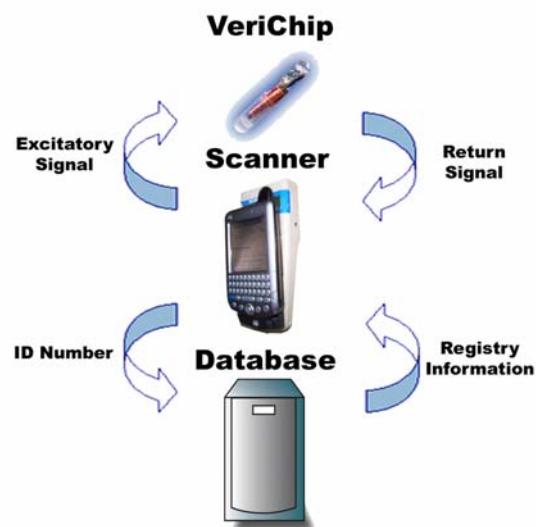


Figure 3. A VeriChip system. A schematic showing how a VeriChip system works. Adapted From: <http://www.verichipcorp.com/>

had a VeriChip implanted in his arm and that this particular microchip is tied to a medical database managed by Meriter Hospital. Now suppose it is Halloween weekend and this UW-Madison student is drunk and passes out while walking by himself towards a friend's apartment. He hits his head on the curb. The police find the bleeding student and rush him to Meriter Hospital. In the ER, the emergency technicians immediately want to infuse the victim with blood, but they are unsure of his blood type. Hoping that the man is equipped with a VeriChip, a nurse scans his arm. Within seconds, a list of detailed information including blood type appears on the scanner. The ER doctors now know the intoxicated student's blood type and are able to treat him effectively.

Positive Implications of the VeriChip

Today, consumers already benefit from RFID technologies. For example, the I-Pass allows people to zip through Illinois tollbooths. At Wal-Mart stores, shelves are always well-stocked partly because of the company's RFID-enabled supply chain. The VeriChip will be able to supplement already established RFID technologies, but consumers can benefit in new ways too. Perhaps the largest gains could be achieved in the healthcare sector. For instance, anyone with impaired speech, memory loss or tendencies toward unconsciousness (e.g. narcolepsy) could benefit from a VeriChip that linked to a medical database (<http://www.verichipcorp.com/>). Furthermore, the VeriChip could function as an additional layer of security protection for credit and debit cards (Scheeres, 2003). There are many niche markets where, if properly implemented, a VeriChip system could serve its users well.

The Healthcare Sector

According to Fast Track Technologies—a consulting firm specializing in healthcare RFID technology—the market for RFID technology in the healthcare sector will exceed \$8.8 billion by 2010 (“RFID Use in Healthcare Set to Take Off”, 2005). The VeriChip will certainly be a part of this projected industry spending. In medicine, the VeriChip primarily functions as a tool for managing patient information. Specifically, the chip allows healthcare professionals to quickly and accurately ascertain critical patient information. The device, which contains only a unique serial number, is linked to a patient database maintained by a hospital. Furthermore, the only information stored in the database would be data that the patient approved. Typically, this data would include a person's name, primary physician, family or caregiver contact information, current medications, known allergies, and critical medical history. Again, this personal information would not be stored on the VeriChip but rather in a secure database accessible via the Internet by authorized hospital personnel. To recap, the primary purpose of the VeriChip in the healthcare sector would be for rapid patient identification and medical record access (<http://www.verichipcorp.com/>).

There are a number of key constituents who clearly would benefit from the VeriChip, which as noted previously is typically implanted in the back of the upper right arm.

Anyone with impaired speech, memory loss, or chronic loss of consciousness would benefit from a VeriChip implant (See Figure 4). These conditions create a communication barrier that the VeriChip attempts to remedy. Other chronic illnesses for which the subcutaneous implant may be beneficial include seizure disorders, stroke, diabetes, various cardiac conditions and Alzheimer's disease. All of these ailments may render medical emergencies that leave the victim incapable of communicating critical information (VeriChip Corporation Testimony, 2005). In turn, the lack of communication could delay treatment or even result in medical errors. The VeriChip is designed to convey pertinent information when the patient is unable to do so. In this manner, the VeriChip fills a possible information gap in the healthcare sector, and the device should be considered as a preventative tactic for at-risk individuals. Already, hospitals are accepting the technology. As of October 3, 2005, fifty-eight hospitals across the United States have agreed to implement a patient identification VeriChip system in their emergency rooms ("VeriChip Corporation adds 49 additional hospitals," 2005).



Figure 4. *VeriChip at the hospital.* The VeriChip may be able to provide critical information about unconscious patients who are brought to the ER.
Source: <http://www.safetycenter.navy.mil/>

Why not use a MedicAlert bracelet?

Katherine Albrecht, a vocal critic of arguably invasive RFID technologies, believes that a *MedicAlert bracelet* is a viable alternative to the VeriChip. On her website, www.spychips.com, she cites health cards or bracelets as an alternative to the VeriChip. Proponents of the RFID technology, however, state that the VeriChip cannot be lost, stolen or misplaced—reasons why a bracelet or other information card is often not in the possession of the patient at the time of critical need. As a result, the VeriChip Corporation stands firm in its opinion that its technology is the best way to convey critical patient information. In fact, in a letter to the Congressional Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics, Richard Seelig stated that “the current archaic and inefficient means of managing medical information can be replaced by information systems currently considered routine in all other major business sectors” (p. 9). Seelig—an officer at the VeriChip Corporation—implies that the VeriChip is the next logical step in bringing healthcare practices up to 21st century standards. It seems that the VeriChip, instead of a MedicAlert card or bracelet, may be the next dimension of logistics.

An Additional Layer of Security

A VeriChip also could act as an additional layer of security for high-value assets and credit cards. Already, the Mexican government is using the VeriChip to control access to offices storing sensitive information. Only high-level officials with a VeriChip implant will be able to enter these high-security office suites. The Attorney General of Mexico, Rafael Macedo de la Concha, stated that 18 government officials have received a VeriChip



Figure 5. *VeriChip at the ATM.* The VeriChip could provide an additional layer of security at the ATM.
Source: <http://www.nwresa.org>

implant (Albrecht, 2004). Consumers using credit and debit cards could also benefit from the added protection that a VeriChip offers. According to a study by a MasterCard subsidiary, approximately 50% of debit-card fraud occurs when a family member or friend, who knows the victim's personal-identification number, nabs the card (Sidel, 2005). If a person owned a debit card that required VeriChip authentication in addition to a personal-identification number, then family members and so-called "friends" could not maliciously use a stolen card (See Figure 5). Certainly, the VeriChip would be effective in preventing this type of low-tech theft. ATM machines that utilize RFID technology as a second layer of security are not yet ubiquitous, but many retailers—such as Exxon-Mobil gas stations and McDonald's—are testing RFID enabled credit-card readers in select markets (Scheeres, 2004). It may be only a matter of time before these readers are VeriChip-compatible. Indeed, the VeriChip could serve as an additional security layer for financial transactions.

Special Cases: e.g. Katrina

Healthcare and security are not the only applications of the VeriChip; in fact, the device will likely be used in many other niche markets. One very recent application of the VeriChip is in the field of mortuary science. Imagine that a close relative died in the wake of Hurricane Katrina. You hope to obtain your loved one's remains quickly and bring closure for your grieving family. Unfortunately, the logistical nightmares resulting from Katrina have considerably prolonged your bereavement process. However, a radiofrequency identification chip is helping morticians match and identify victims faster and get their remains back to loved ones quicker. The VeriChip—implanted in the deceased after death—can be used to keep track of human remains, speed up the morgue-

management process and reduce morticians' errors. In fact, Gary T. Hargrove, coroner of Harrison County in Mississippi, stated, "[The VeriChip has] better enabled me to do my job as the coroner—tracking and getting people's loved ones back to them quickly" (Dishneau, 2005, p. 1). Indeed, the VeriChip has proved to be a boon in the aftermath of Katrina. Of course, this example is only one application of the technology—and a rather macabre one.

Negative Implications of the VeriChip

Undoubtedly, the VeriChip has beneficial uses; yet, there is a great deal of opposition to the technology. Katherine Albrecht, considered the nation's leading expert on consumer privacy, recently coauthored the best-selling book, *SpyChips*. In this account, Albrecht specifies how corporations use RFID technology to track shoppers and build detailed consumer profiles. This increased surveillance—and reduced privacy—have many people worried. The VeriChip could be another step toward a "Big Brother" society (Cavoukian, 2005).

Will Privacy be Lost?

Perhaps the largest concern regarding the VeriChip is the potential loss of privacy that ubiquitous use of such a device might create. Critics constantly name loss of privacy as the primary rationale against the *biometric device*. In an analysis of privacy issues and biometric technologies, Clyde Wayne Crews Jr.—the director of technology studies at the Cato Institute—cites database aggregation as a major cause of this privacy loss. A VeriChip system, which stores identifying information in a database, creates yet another catalog that could be broken into by identity thieves, merged with other databases or simply used unethically (Crews, 2002).

Interlocking databases remain a concern with respect to VeriChip



Figure 6. Databases and the VeriChip. Implementing a VeriChip system will require large databases of consumer information. Will these catalogs of information be used ethically?

Source: <http://www.domainmasters.net/>

systems (See Figure 6). The database that stores the personal information tied to the VeriChip's serial number is arguably the most critical part of a VeriChip system. Opponents of the device contend that these VeriChip databases may become linked to other private and public databases. Indeed, merging information from multiple databases has become a lucrative business. These interlocking databases make complete profiles on any consumer available. Such biographical sketches might include name, address, social security number, credit reports and—with the addition of VeriChip databases—even medical records. For example, ChoicePoint Inc., a *data broker*, aggregates and sells personal information to insurance companies, firms looking for improved marketing insights and even the federal government. The company tracks information regarding consumer behavior and maintains databases with names, social security numbers and credit reports. With over 10 billion records, the company stores information about virtually every consumer in the United States (Sullivan, 2005). Bruce Schneier, a security expert, predicts that companies such as ChoicePoint will start maintaining databases of RFID numbers and their associated people (Schneier, 2005).

Unfortunately, these aggregate databases are a tempting target for criminals. In February, ChoicePoint accidentally sold confidential information on 145,000 people to identity thieves posing as legitimate businessmen (Conkey, 2005). And database breaches have become more and more common in the last few years. Introducing the VeriChip creates the potential for a person's medical history to be included in these cumulative databases. In fact, in November, the U.S. Senate passed the *Wired for Health Care Quality Act*, which recommends a partnership between the government and business to modernize information technology resources in the healthcare industry. The VeriChip Corporation is one company that the government sees as a potential partner. Critics insist that the Senate bill incorporates only lackluster security measures. For instance, they mention that the bill fails to control for who can and cannot access these to-be-created databases. What if employers accessed the databases to help make promotion and hiring decisions (White, 2005)? In the end, consumers have little reassurance that VeriChip databases will remain private and separated from other databases and data brokers. Consumers considering the VeriChip should be wary as their personal information will be at the discretion of whoever controls the accompanying VeriChip database.

What is the VeriChip Corporation Doing about Privacy?

To combat rising concerns regarding their technology, the VeriChip Corporation crafted a careful *privacy policy*. In a letter to the Congressional Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics (NCVHS), the VeriChip Corporation outlined its guiding privacy principles. In this privacy policy, the VeriChip producers emphasize that only the VeriChip customer may decide what groups can access his or her database information. The company appears very concerned with privacy; it has even appointed a Chief Privacy Officer and pledges to keep privacy matters a top priority (VeriChip Corporation Testimony, 2005). But simply drafting a privacy policy and appointing a privacy officer may not be enough. Nevertheless, the company vows to keep privacy a chief concern.

What about Health Risks?

While the VeriChip Corporation touts its device as completely safe, critics cite a number of health risks associated with the chip. On October 12, 2004, the FDA approved the VeriChip for human use (<http://www.epic.org/rfid/verichip.html/>). Specifically, the federal watchdog group categorized the device as a *Class II device*. Being a Class II device, the VeriChip is subject to a number of additional safety standards relating to tissue compatibility, *magnetic resonance imaging (MRI)* compatibility and overall performance (FDA: Class II Special Controls Document, 2004). In addition, the FDA (Donna-Bea Tillman, personal communication, October 12, 2004) outlined a full list of health concerns regarding the device in a letter sent to the makers of the VeriChip:

“The potential risks to health associated with the device are: adverse tissue reaction; migration of the implanted transponder; compromised information security; failure of implanted transponder; failure of inserter; failure of electronic scanner; electromagnetic interference; electrical hazards; magnetic resonance imaging incompatibility; and needle stick (p. 3).”

These health hazards—like “migration” and “needle stick”—sound appalling. With all these risks, why would anyone choose to receive a VeriChip implant? Well, the aforementioned hazards are primarily worst-case scenarios; indeed, most people with a VeriChip will not have to worry about the device migrating from their arm to their leg. Still, potential risks such as compromised information security and magnetic resonance imaging incompatibility *should* be



Figure 7. Health Risks and the VeriChip. People with a VeriChip would be unable to undergo an MRI procedure. Source: http://www.williamoslerhc.on.ca/Patient_Services/

alarming. MRI, for instance, is a common imaging technique used to diagnose all sorts of diseases—the procedure can be life-saving. Opponents of the VeriChip cite this incompatibility as a rationale against the device (See Figure 7). Katherine Albrecht, an expert privacy advocate in the RFID world, puts the device into perspective on her website: “If it’s a choice between a potentially life-saving diagnostic procedure or a VeriChip implant, I believe most patients would choose the MRI” (Albrecht, 2004a). As an alternative, Albrecht recommends wearing a MedicAlert bracelet because it circumvents all of the health risks of the VeriChip, and emergency technicians know to look for it. While most potential health risks outlined by the FDA should not cause

consumer angst, big issues like MRI compatibility and information security should be of concern to people considering the VeriChip.

How Secure is the VeriChip?

Although the VeriChip Corporation insists that its device is completely secure, experts are compiling evidence favoring the contrary position. Yes, the VeriChip will act as an additional layer of security in many applications; but, as with almost any technology, the VeriChip is still “hackable.” Scott Silverman, CEO of the VeriChip Corporation, has promoted his company’s RFID technology as a security tool. He claims that the VeriChip is secure because it only transmits a unique serial number that, by itself, means absolutely nothing. But Bruce Schneier, a security expert, disagrees. Alluding to the VeriChip, Schneier (2005) states:

“Even a chip that only contains a unique serial number could be used for surveillance. And it’s easy to link the serial number with an identity—when you buy the item using a credit card, for example—and from then on it can identify you” (p. 1).

In this quotation, Schneier suggests that clandestine parties could track VeriChip users. The fundamental technical problem lies in the design of RFID technology. Currently, most RFID tags can be uniquely identified by their *collision avoidance signal*—a special identification number that lies deep within the chip’s architecture and has nothing to do with the chip’s transmission data. The collision avoidance signal, as the name implies, allows an RFID scanner to work when there are multiple RFID tags within range of the scanner. When many tags are in range of a scanner, each tag behaves uniquely based on its collision avoidance signal. In this way, the scanner knows which chip is which. Researches have already developed a method for identifying chips based on this activity. Thus, Schneier believes that current RFID technology, like the VeriChip, is far from secure. Schneier proposes a fix to this problem; he suggests basing the collision avoidance protocol on a random number instead of a static number—a specification known as ISO 14443A (Schneier, 2005). While this high-tech approach to cracking the VeriChip may seem far-fetched, it is still plausible. If a savvy criminal really wanted to steal—or mimic—a person’s VeriChip, it could be accomplished by reading and replicating the device’s transmission data and collision avoidance signal. Before savvy consumers adopt this technology, they will likely demand that the VeriChip be made more secure—perhaps by encrypting the verification number and using a new collision avoidance standard.

A VeriChip on Society’s Shoulder

With the VeriChip, there is the potential for social gains but also for personal loss of autonomy. While emergency room patients and consumers seeking convenience may reap immediate rewards from VeriChip systems, the very same people and others may

experience a considerable reduction in individual privacy. Is this potential invasion of privacy worth the extra convenience that the VeriChip offers? In the next few years, policy makers in the United States will have to make a decision about whether or not to accept the VeriChip technology. Some pessimists say the VeriChip is another step in the creation of a “Big Brother” society—a dystopia—where central bureaucrats have the ability to track and catalog our every move. Already some school children in a Sutter, California elementary school are required to wear RFID tags to mechanize attendance-taking and reduce vandalism (Leff, 2005). Where will RFID tags, such as the VeriChip, be implemented next? Despite the VeriChip’s small size, society’s coming decision looms large.

So what will happen? It is the opinion of this author that RFID technology will eventually become the primary mode for accessing patient records in the healthcare sector. The VeriChip will likely be the specific tool that hospitals and clinics choose to use for this purpose. Within ten to twenty years, it is probable that every major hospital in the country will be equipped with a VeriChip system. Already, the VeriChip Corporation’s technology is poised for widespread use. In fact, the company has agreements with over 50 hospitals to employ a VeriChip system. With the passing of the Wired for Health Care Quality Act—a Senate bill that funds joint government-business initiatives for digitizing medical records—the VeriChip seems well-positioned to break into the healthcare sector. If the device is used only in this respect—and databases containing patient information are kept secure—then the device can certainly have a positive effect on society.

Yet problems with the VeriChip may arise if companies use these databases to track consumers or build extensive profiles about them. This information would be an attractive target not only for identity thieves but also for companies seeking to analyze consumers. People need to be wary of the risks associated with the VeriChip—namely, the possible reduction in personal privacy. Certainly, most people with a VeriChip implant would not be targets of surreptitious tracking. Still, people will likely lose some privacy because more complete information profiles can be created with the implementation of a biometric device like the VeriChip. In the coming years, many concerned privacy advocates will fight for safeguards against biometric devices such as the VeriChip. Their efforts to limit how such technology may be used will be critical in how the VeriChip impacts society. It will be interesting—and perhaps pivotal to personal privacy rights—to see how the VeriChip story unfolds.

Glossary

Active RFID tag — a RFID tag that contains its own power source

Biometric device — an authentication technology that uses a biological aspect of an individual to grant access to a secure service

Class II device — a Class II device requires special controls such as performance standards and after-market observation

Collision avoidance signal — a uniquely identifying signal sent by an RFID tag; this signal is used to identify a particular RFID tag when many tags are in range of a scanner

Data broker — a company that aggregates database information and sells the accumulated information to other organizations

Inductance — the physical property of a circuit by which a current is produced to oppose a change in magnetic flux

Interlocking databases — two or more databases that are linked together; provides more complete information about a subject

Magnetic resonance imaging (MRI) — a diagnostic procedure in healthcare that uses high-frequency radiation to detect varying nuclear spins in the body's hydrogen atoms; from these differences, a detailed image of the scanned person's internal tissues is created

MedicAlert bracelet — bracelet imprinted with critical medical information about the wearer

Radiofrequency identification (RFID) tag — an identification label that transmits information using radiowaves

Passive RFID tag — a RFID tag that does not contain its own power source

Privacy policy — a statement of a company's guiding principles regarding how the company uses information collected from a consumer

Wired for Health Care Quality Act — a bill passed in the U.S. Senate on November 18, 2005; provides grant money to research institutions and businesses for developing technologies that can streamline healthcare information technology systems

References

- Albrecht, K. (2004a, October 19). *FDA letter raises questions about VeriChip safety, data security*. Retrieved November 23, 2005, from <http://www.spychips.com/press-releases/verichip-fda.html>
- Albrecht, K. (2004b, November 29). *VeriChip RFID implants in Mexican Attorney General's Office Overstated*. Retrieved November 23, 2005, from <http://www.spychips.com/press-releases/mexican-implant-correction.html>
- Appell, D. (January 2003). Getting under your skin: Safety questions about implantable chips persist. *Scientific American*, 18-20.
- Banker gets ID chip implant. (2005, September 19). *Red Herring*. Retrieved October 23, 2005, from <http://www.redherring.com/Article.aspx?a=13649&hed=Banker+Gets+ID+Chip+Implant>
- Cavoukian, A. (February 2004). *Tag, you're it: Privacy implications of radio frequency identification (RFID) technology* (2004). Toronto; Canada: Information & Privacy Commissioner/Ontario.
- Conkey, C. (2005, November 26-27). Identity-theft bills stall in Congress. *The Wall Street Journal*. p. A4.
- Crews, C. W. Jr. (September 2002). Human bar code: Monitoring biometric technologies in a free society. *Policy Analysis*, 452, 1-20.
- Dishneau, D. (2005, September 28). Chips help coroners keep track of hurricane victims. *USA Today*. Retrieved October 10, 2005, from <http://www.usatoday.com>
- Food and Drug Administration. (2004). *Class II special controls guidance document: Implantable radiofrequency transponder system for patient identification and health information*. Retrieved on October 17, 2005, from <http://www.fda.gov/cdrh/ode/guidance/1541.pdf>
- Fox, S. (2004). Innovation: Getting chipped. *Journal for the Arts, Sciences, and Technology*, 01, 74-85.
- Garfinkel, S. & Holtzman, H. (2005). Understanding RFID Technology. In, *RFID: Applications, Security, and Privacy*. (1st ed., pp. 15-22). Addison Wesley Professional.
- Leff, L. (2005, February 11). In California, RFID tags required for Brittan Elementary School students. Retrieved on October 24, 2005, from <http://www.securityinfowatch.com/article/article.jsp?id=3029&siteSection=306>

- Murray, C. J. (2004, July 26). Implantable chips get under skin of security experts. *Electronic Engineering Times*.
- RFID use in healthcare set to take off. (2005, April 26). *RFID Journal*. Retrieved November 25, 2005, from <http://www.rfidjournal.com/article/articlprint/1534/-1/1/>
- Sidel, R. (2005, October 17). Identity-theft Unplugged. *The Wall Street Journal Campus Edition [The Badger Herald]*. p. 11.
- Scheeres, J. (2003, November 25). When cash is only skin deep. *Wired*. Retrieved October 16, 2005, from <http://www.wired.com/news/technology/0,1282,61357,00.html>
- Schneier, B. (2005, November 3). Fatal Flaw Weakens RFID Passports. *Wired*. Retrieved on November 3, 2005, from <http://www.wired.com/news/privacy/0,1848,69453,00.html>
- Sullivan, B. (2005, February 14). Database giant gives access to fake firms. Retrieved November 26, 2005, from <http://www.msnbc.com/id/6969799/print/1/displaymode/1098/>
- VeriChip Corporation Testimony to the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and health Statistics (NCVHS) regarding the Privacy Issues Raised by the Use of RFID Technology in Healthcare Settings Especially in the Context of the NHII, 109th Cong., 1st Sess. (2005) (testimony of Richard Seelig).*
- VeriChip Corporation. (2005, October 3). VeriChip Corporation adds 49 additional hospitals during month of September that have agreed to implement the VeriMed™ Patient Identification System.
- White, E. (2005, November 20). Senate urges using tech for medical records. *USA Today*. Retrieved November 27, 2005, from <http://www.usatoday.com>