FLASHPOINTS AND CONTROVERSIES

The use of RFID technology in security and health applications will raise few problems, as they'll represent layers atop existing monitoring systems, or uses in context where people already expect to give up a measure of privacy. However, other application areas hold the potential to generate controversy about RFID, or opposition to its further deployment. Three in particular stand out: RFID use in libraries; in government IDs like passports and drivers' licenses; and in medical or security implants.

Underlying each of these uses is another question: is RFID secure enough for applications in which tags are taken out of controlled environments like casinos, amusement parks, airports, and hospitals, and used in high-stakes applications like government IDs and credit cards?

This memo considers each of these three application areas, and the question of RFID security. It does so to point out that while RFID holds great promise as a technology that can increase convenience for shoppers, serve as a platform for development of new services, and ultimately serve as one of the building blocks of pervasive computing, it could also fail to live up to its potential—if we aren't smart about how it's used in the near term.

A SERIES OF MEMOS ON RFID

To help Technology Horizons Program members understand the long-term potential of RFID, the Institute for the Future (IFTF) has undertaken a project to map the future of RFID beyond the supply chain. Even though companies are struggling with the Wal-Mart and Tesco mandates to add RFID tags to pallets and cases of goods, it's not too early to begin thinking about how the technology could be used outside the supply chain. Our findings are presented in a series of five memos. The first memo, Thinking About RFID (SR-926A) explains what RFID is and how it has evolved. The second, Public Concerns and the Near Future of RFID (SR-926B, analyzes consumer concerns about RFID, and discusses recent and coming controversial uses of the technology. This memo, **Flashpoints and Controversies** (SR-926C), the third in the series, focuses on controversial potential uses of RFID. The fourth, Smart Homes and Sociable Devices: RFID Takes Off (SR-926D), looks at RFID's role in smart homes and a world of pervasive computing. And in the fifth and final memo, RFID: Implications and Recommendations (SR-926E), we discuss what the future of RFID means and how to avoid potential pitfalls posed by controversial uses and navigate to a world where businesses and consumers alike find great value in RFID.

LIBRARIES AND RFID

A number of libraries in the United States have installed RFID systems, and many more are considering investing in RFID projects. Such systems are appealing for several reasons. They promise to streamline check-out and check-in of books, reduce lost time among library staff due to repetitive stress injuries. They make library inventory easier: indeed, some large university libraries never conducted exhaustive inventories before installing RFID systems. They also speed identification of misplaced books.

A small number of publishers are also starting to offer RFID-tagged books. In 2004, Dutch publisher NBD Biblion announced that it would tag all its books, while Blackwells and Baker & Taylor offer library buyers the option of buying pre-tagged books.

Deployment and debate over RFID use in libraries will probably play a role in shaping public perception of RFID. Libraries are ubiquitous institutions in American society. Librarians have long advocated privacy protection for patrons, and users have high expectations regarding the privacy of their records.

RFID TAGGED GOVERNMENT IDS

A number of governments, including China and the United States, plan to use RFID in drivers' licenses, passports, and other government IDs in the next several years. The details of these deployments are still murky, but the use of RFID in government identification could create serious problems for the technology's public image.

The push in the United States to put RFID in drivers' licenses and passports is part of a broader campaign to update and secure government-issued IDs. This effort, which includes tightening procedures for applying for licenses, and standardizing license designs at the state level (there are currently some 200 different designs for legal drivers' licenses in the United States) has been going on for some years, but took on a new urgency after 9/11. The Virginia General Assembly's House Science and Technology Committee, in an effort to make its drivers' licenses less prone to falsification or abuse (several of the 9/11 hijackers carried Virginia drivers' licenses), recently held hearings on the pros and cons of RFID-embedded licenses. (Similar proposals to create smart licenses failed in Utah in 1996, New Jersey in 2000, and New Mexico in 2001.)

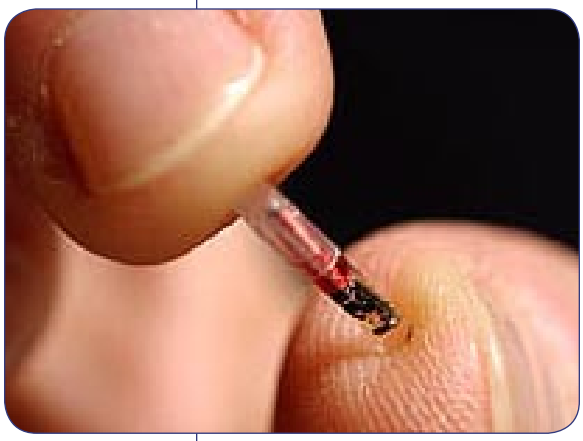
Plans to create a new generation of RFID-embedded passports have also been controversial. The International Civil Aviation Organization (ICAO), a Montreal-based group that sets standards for passport design, began work in 2003 on a new generation of machine-

readable passports. However, critics have raised technical, security, and political objections to using RFID in passports. Some security experts contend that the proposed standard trades security at the expense of global operability: in its quest to make it easy for customs officials to read tagged passports, ICAO has sacrificed too much user privacy. Finally, liberals and libertarians alike see tagged passports and drivers' licenses as potential tools for infringing on domestic civil liberties.

IMPLANTS

Implanted tags—RFID tags injected subdermally in people—are in their infancy. Implanted tags have potential uses in health and security, but raise concerns about privacy and government surveillance greater than those in passport or clothes tagging. RFID tags have been injected into pets for over a decade. The tags contain a unique ID number that, when entered into a database, provides information about an animal's owner and address.

In October 2004, the FDA approved implantation of Verichip's Digital Angel RFID tags in humans for medical purposes. Essentially, each tag will be a pointer to a database, allowing hospitals to retrieve electronic records on patients, even those who arrive unconscious or unable to communicate. A few people, most notably the Mexican Attorney General and his top staff, have had RFID tags implanted as part of a system to restrict access to sensitive areas and documents. Finally, at least one business, the Baja Beach Club in Barcelona, offers subdermal RFID tags to patrons as a cashless card and pass to restricted portions of the club.



Source: USA Today

It is too soon to tell how successful these projects will be, or whether they will overcome public skepticism. The Verichip tags require proprietary readers, and the company plans to offer the tags as part of a subscription-based service: in other words, emergency rooms will be able to access information about you only if your membership in the Digital Angel service is still active. In the cast of the Mexican Attorney General's office, implanted chips are essentially used like security badges: their purpose is to protect secure areas and materials from people, not to protect people from attack. (Indeed, according to CASPIAN, one Mexican kidnapping gang has defiantly renamed itself "el chip.")

It also appears that chip implants have yet to win over the public. A 2004 April Fools' article about a U.S. government plan to implant RFID in homeless people provoked an outcry on government conspiracy Web sites. An edited version surfaced in Australia a few months later, and continues to circulate.

Public Concerns and the Near Future of RFID

IS RFID SECURE ENOUGH?

Some security experts worry that RFID tags used in government IDs and contactless credit cards are not secure or robust enough. If their fears turn out to be well-founded, they could seriously affect public perceptions of RFID.

There are some now well-known examples of commercial RFID tag encryption being hacked: students at the Johns Hopkins University's Information Security Institute, for example, recently managed to break the encryption on the tags used in Mobil's Speedpass system. Visa plans to introduce a credit card with an encrypted chip later this year; so far, it remains unbroken.

Library RFID systems currently are designed with no more security than exists with traditional library systems. But as computer scientist David Molner recently argued, using RFID-tagged books to track people would be extremely labor-intensive but not impossible. Authorities might compile lists of suspicious books' RFID tags, and monitor library exits for signs that those books have been checked out; but they would have to compile lists for each library they wanted to monitor, as each RFID tag in each book is unique.

The biggest concerns focus on RFID-enabled government IDs. The standards for these tags sometimes don't even include encryption, on the grounds that leaving tags unencrypted will make it easier for law enforcement to adopt and use the technology. Unfortunately, however, this also raises the possibility that hackers, data thieves, or terrorists could also read the data on IDs. (See text box, "RFID in Passport Security")

Security analysts worry about other elements of the RFID system. Readers may have less security built into them as tags. Tom Kellerman, a security expert with the World Bank, recently laid out some of the dangers: RFID readers are spoofable, the 40-bit encryption algorithm currently used on tags can be cracked, and man-in-the-middle attacks are possible. More generally, wireless systems are always harder to secure than wired ones: eavesdropping is impossible to avoid in wireless communication, forcing designers to rely more heavily on encryption, frequency-shifting, or other means to avoid detection and deciphering.

RFID IN PASSPORT SECURITY

For over a decade, passports have supported optical character recognition (OCR); the bottom of the inside cover of your passport—the page with your photograph—probably has a two-line "machine readable zone," designed to be read easily by an optical scanner.

OCR systems have helped speed immigration control—countries that want their citizens to enter the United States without visas must issue OCR-readable passports—and standardization of customs practices. Just as RFID reduces media breaks in business, so too does ICAO see potential to reduce them in travel: "global interoperability of MRTDs [machine-readable travel documents]," it argues, "promotes facilitation in international travel and generally enhances security, especially aviation security." ICAO considers contactless cards to be the next logical step in machine readability. Given the growing volume of international travel, and the desire in the travel industry to keep security and customs delays to a minimum, adding some smart card features to passports makes sense.

Critics argue that ICAO specification leaves the data on the passport relatively insecure—less secure than credit or ATM cards. The chips will have measures to guarantee that they have not been altered or rewritten, but they will not be encrypted; this will make it easier for third parties to read passports. (According to *Wired News*, "Security experts said the U.S. government decided not to encrypt the data because of the risks involved in sharing the method of decryption with other countries.")

ICAO specification also leaves passports vulnerable to counterfeiting. The chips will contain digital versions of the bearers' biometric information and pictures, but not their signature. Consequently, technology and travel writer Edward Hasbrouck argues: "An identity thief, using only the data secretly and remotely obtainable from your passport, will be able—without ever having actually seen you or your passport—to create a perfectly valid-seeming passport, with a valid encrypted and properly signed digital hash, with your photograph but a signature in their handwriting."

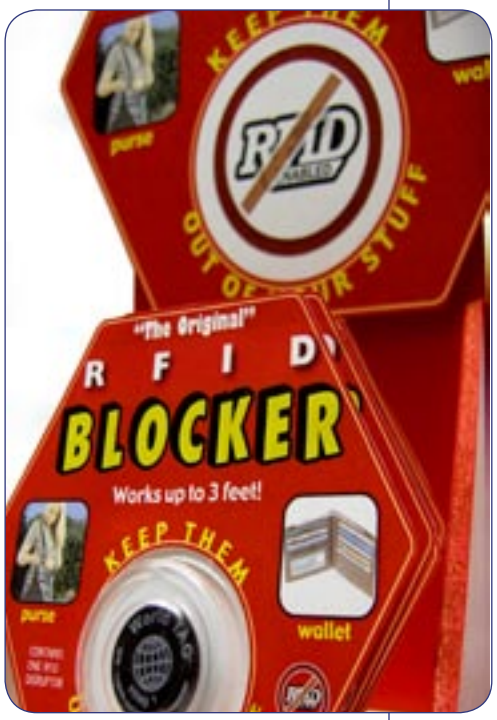
Such a document is the holy grail of identity thieves, organized criminals, money launderers, and, or course, terrorists.

Inadequate encryption, Bruce Schneier argues, makes RFID-embedded passports a safety risk to travelers, since "pickpockets, kidnappers and terrorists can easily—and surreptitiously—pick Americans or nationals of other participating countries out of a crowd." They would also give foreign governments a tool for conducting surveillance against Americans. "It is a clear threat to both privacy and personal safety," Schneier concludes, "and quite simply, that is why it is bad idea."

Finally, some privacy and civil rights advocates worry that tagged passports and drivers' licenses will make government surveillance easier. The ACLU's Barry Steinhardt declared, "By instituting RFID chips in passports, the U.S. government could skip right over the politically untenable proposals for a national ID card, and set a course toward the creation of a global identity document—or, at least, toward a set of global standards for identity that can be incorporated into a wide variety of national identity documents. ... Developed without outside input, the ICAO passport has morphed from a simple identity document to become a de facto monitoring device."

Public Concerns and the Near Future of RFID

Consumer backlash to RFID could occur around government applications of the technology, such as in libraries and passports.



If consumers feel a lack of control over their RFID-enabled products, they may resort to alternative solutions that offer protection form invisible intrusion. This is what one of these alternatives might look like: an RFID tag that disrupts all RFID signals in a small area.

THE NEGATIVE SCENARIO

What happens if these issues aren't settled? The fourth memo in this series, *Smart Homes and Sociable Devices: RFID Takes Off* (SR-926D), will outline a future of "smart homes and sociable devices," in which people find they can trust RFID technology, and have the ability to create new services and uses by extending the abilities of tags, readers, and software. And in the fifth and final memo of the series, *RFID: Implications and Recommendations* (SR-926E), we'll describe in detail some recommendations for how to reach such a future, by making sure that users have the ability to innovate around RFID.

But it's worth pausing to think about what a future in which RFID is tightly controlled and not trusted would be like. What happens if tags on IDs turn out to be insecure, or if companies and governments actively work to maintain control over RFID and discourage user innovation? In such a world, trusted RFID applications remain limited, both because of limitations in the technology, and the inability of users to develop and share defenses against or corrections to them. RFID uses in airports or amusements parks, instead of showcasing positive uses of the technology, become isolated examples of responsible use. The following "articles from the future" illustrate how this negative scenario could unfold.

Richmond Times-Dispatch **September 2, 2008**

Muft Card CEO Resigns Amid Security Problems

By C. K. Kahn

Marvin R. Stennet III, the CEO who in a few short years turned Infocredit into a fast-rising player in the credit card world, resigned yesterday.

Jennifer Cabal, a spokeperson for Infocredit, said that Stennet "decided the time was right to spend more time with his family." Sources close to the family say that they have left for "a time of reflection and prayer" in the Bahamas. Calls to Stennet's lawyer, C. Vann Midlothian, were not returned. A secretary, who refused to give her name, said that Mr. Woodland had left for "a time of reflection and prayer" at an undisclosed location.

Infocredit's Muft Card, which was the fastest-growing credit card in North America, became the subject of intense scrutiny this summer when it was revealed that high-tech thieves had learned how to read the RFID chip on the card, and access the owner's account information. Muft is a Hindi word meaning "free-of-cost;" Infocredit had aggressively targeted immigrant and low-income communities, and kept its fees low by selling customer information.

According to FBI reports, in 2007 computer criminals discovered a flaw in the encryption algorithm used on the card, which allowed them to access personal information on Muft cards. This information, in turn, was used in online purchases, or written onto counterfeit cards.

Security experts had warned that the encryption standards for RFID-enabled credit cards—or "contactless convenience cards," as the industry prefers to call them—were inadequate, and that large-scale fraud was all but inevitable.

"Look, it's all wireless. That means it can be hacked. Period," said Michael Hertzberg, a graduate student at Johns Hopkins University's Information Security Institute and author of the blog StealThisCard.typepad.com. "The encryption problems have been common knowledge for a couple years. It's just amazing this didn't happen before."

Visa and Mastercard, which also have RFID-embedded cards, insist that their cards are secure. Visa insists that the recent spate of card fraud in China was the fault of database subcontractors in Korea.

Critics say that the fundamental problem is that the convenience of contactless cards, which don't require signatures, trade security for convenience. "In their desire to replace cash, Infocredit and the rest of the industry have sacrificed too much security for ease of use," Simson Garfinkel, a columnist and technology consultant, said. "Security requires proving who you are, and having your identity and your card's identify verified. Infocredit redefined all that as inconvenience, and did away with it."

"In their desire to replace cash, Infocredit and the rest of the industry have sacrificed too much security for ease of use,"

The Muft card had positioned itself as a card for young adults with fast lifestyles that would be cramped by conventional cards. The company had also been criticized by religious groups for its risqué "Get Muf't" ads, which combined elements of Bollywood, Hong Kong action cinema, and hip-hop.

Because of the Infocredit debacle, consumer advocates are warning people to avoid all RFID-tagged cards. "There's a simple way to protect yourself: don't use them," Baxter Bailey, head of the Digital Consumer Protection Agency, said. "That's getting harder and harder, but you can still find smaller banks that don't yet issue chipped cards."

Infocredit's problems also are raising broader questions about the viability of RFID tags in financial and government services. In November 2006, al-Qaeda member Sulemin al-Fatmid (formerly Warren Jones) penetrated the E-ring of the Pentagon with an RFID-enabled ID badge that identified him as former Defense Secretary Donald Rumsfeld. In the summer of 2006, a computer error briefly resulted in all carriers of RFID-enabled passports at Chicago's O'Hare Airport being flagged for strip searches and FBI questioning.

"The question now is not whether RFID should be used in these contexts," futurist Paul Saffo said. "It's whether the rest of the RFID industry can survive the fallout."

The Infocredit scandal has rocked Richmond, which has emerged as a rival to Atlanta as a financial center.

Stennet was at one time a pillar of the Richmond business and social world. His marriage to a former Miss Virgina who hailed from one of the state's "First Families," Infocredit's rapid growth, and his recent campaign to have a statue of himself added to Richmond's Monument Avenue, all drew considerable attention.

Now he has few supporters left in the city.

Roger "Lefty" Washington, an Infocredit customer whose account was charged $34,000—more than Mr. Washington's annual salary as a janitor at Henrico High School—said, "He'd better spend some time with his family, because they ain't gonna want to visit him in the jail he's going to."

Henrico cafeteria supervisor Melvia Thompson had another explanation. "It's just more proof that these chips are the Mark of the Beast," she said. "As if anyone needed any more proof, what with the U.N. using them on them black helicopters," she added.

Navigation

Main Page
Community Portal
Current Events
Recent Changes
Random Article
Help/Contact Us
Donations

Search

GO SEARCH

Tool Box

What Links Here
Related Changes
Upload Files
Specific Pages
Printable Version

StealThisCard.typepad.com/2009/3/17/stupid_stupid_s.html

March 17, 2009

STUPID, STUPID, STUPID

Well, it happened. The government and credit card industry, desperate to keep the lid from blowing completely off its bad RFID tags, haven't taken the high road and tightened the encryption standards. They haven't open-sourced the standards, so serious crypto freaks could fix them. And they're not trusting entrepreneurs to come up with new tools to plug the holes.

No, they attacked the problem by banning personal RFID readers.

Just in case anyone in the free world hasn't seen the article, the always-on-the-ball C.K. Kahn has the story:

FCC Bans Home RFID Readers
Consumer Advocates Divided While an Industry Scrambles
Special to the *Washington Post*
By C.K. Kahn
March 16, 2009

In a surprise move, the FCC yesterday issued new regulations banning personal ownership of RFID (radio frequency identification) readers, and technologies to block RFID readers.

FCC Commissioner Tom Davis, speaking to the press after the contentious vote, said, "Today's decision by the FCC is a brave stand against terrorism, privacy violations, and illicit uses of a promising technology that liberals and Luddites have attacked relentlessly."

The new rules outlaw RFID readers, radio devices that communicate with RFID tags.

The Frist Administration, which had pushed for the ban in the wake of last year's Infocredit scandal and earlier problems with RFID-embedded government IDs, hailed the decision as a victory for consumers and the general public.

White House press secretary Dennis Miller said, "This ban will ensure that children won't be snatched off the streets by RFID-reading pedophiles, that Grandma won't have to worry about her painkillers being read by drive-by drug crazies, and that al-

Qaeda can't make fake passports. It's a good day for America."

The regulations had been opposed by retailers who saw the new rules as overly restrictive, and by companies marketing RFID readers and software for use in the home. However, the regulations passed after a last-minute compromise that gave companies with "prior relationships" with consumers to deploy RFID readers in public places. Pharmaceutical and insurance companies also won an exemption for smart medicine chests, which are expected to reach the market later this year.

However, the new language appears to do nothing to help companies selling readers for home use, in cars, or for tracking personal items. Technology and patent lawyers contacted for this article said that it appears to outlaw personal possession of an RFID reader, as well as technologies like "blocker tags" and insulated bags, and "Faraday cage" devices.

Critics of RFID use in credit cards and government IDs, privacy advocates, and computer industry insiders denounced the new regulations.

"It's the beginning of the end for good RFID," Francis O'Hanlon, CEO of HomeTag, a company making RFID tags and readers for personal use, said. "This ruling means that a promising technology that could have helped millions of people, and spurred a new wave of innovation, will remain in the hands of states and corporations."

Lucian Chen, director of Google's @Home research initiative, said, "These regulations won't do anything to fight crime or prevent terrorism. They'll do is keep people from being able to use RFID, without protecting them from abuses of the technology."

Harvard law and engineering professor Michael Neely, who argued against the legislation, wrote on his blog, "With a single blow, this kills off one of the most interesting set of bottom–up, user-driven innovations we've seen in the last 20 years. This wasn't just remix culture: it was a remix of cyberspace and the real world that promised to redraw the boundary of bits and atoms."

"The stakes are higher than the FCC realized," said Paul Saffo, a research director at the Institute for the Future, a California think-tank.

"Until yesterday, RFID tags were part of a big, exciting brew of technologies that were poised to merge the physical world and cyberspace," he said. "The ability of ordinary people to attach digital information to anything was a key component of the coming world of pervasive computing. We can forget that dream."

Neely and Saffo have it right. This decision kills off an industry, benefits entrenched interests, and protects people who've screwed up RFID from being held accountable for their mistakes. It's like a bank publishing credit card and checking account numbers of its customers, then getting the government to ban Web browers.

But the deeper problem is that it aborts a whole world of innovation that could have been as exciting, as decentralized, and as user-driven as the Internet. Meanwhile, in Denmark and Sweden they're teaching kids how to hack together readers, and encouraging them to tag everything in their schools. The teachers aren't doing this, and the education ministries swear that they aren't using the technology themselves; they're letting the kids build this world for themselves, and learn how to live in it. They're getting valuable lessons in how you shape technologies, and that you can shape them.

Special to the Seattle Times **April 13, 2010**

Health Insurer Cancels Policy Because of Vacation

By C. K. Kahn

Case shows complicated balancing act between information privacy, reporting, and regulation

SEATTLE--Mark Greenberg returned from a two-week camping trip in the Rockies to find a pile of mail, a few withered plants—and his health insurance cancelled.

The Tacoma resident has allergies and chronic illnesses that require a variety of drugs. He uses a smart medicine cabinet to help him keep track of the various medicines he has to take. The cabinet communicates with Greenberg's cell phone and alarm clock to remind him when it's time to take medicines, and to warn him away from combinations of drugs that could be dangerous. The cabinet also sends information about Greenberg's track record to his health insurer, Healthwatch.

And that's where the problems started.

When Greenberg went camping in March, he says he printed out his drug schedule, and took his medicine with him. But Healthwatch says that since it has no record of Greenberg's following his prescribed drug regimen, they can cancel his insurance.

"Patients failing to finish their drug treatment courses present a giant problem to health providers and payers, and ultimately to society at large," says Kevin Marburg, a representative for Healthwatch. "Billions of dollars are wasted on drugs that aren't finished, and billions more are wasted on additional treatments made necessary by patient misbehavior."

He later added in an e-mail, "Healthwatch remains committed to providing the highest-quality, most responsive financial solutions for managing health. But it can only achieve its goals, and create value for doctors, patients and investors if the user is an active, willing partner in the process."

Healthwatch drew considerable attention last year for its advertising campaign, which featured the slogan, "We watch, you benefit."

"Mr. Greenberg is upright and healthy, not in an ICU," Kim Yong Tok, Greenberg's attorney, says. "Given the variety of conditions he has to manage, that's proof that he kept to his meds."

Ultimately, however, Healthwatch's decision is based not just on whether Mr. Greenberg kept to his regimen, but whether Healthwatch possesses the electronic data showing that he did.

The Healthwatch system, which is similar to those offered by Medview, Wesee Health, and other insurers, consists of several parts. The smart cabinet contains an RFID reader that "interrogates" the RFID tags on medicine bottles as they are removed and returned. It also connects to a health provider database, which keeps track of the course of drug regimens and sends alerts and reminders to subscribers.

The system communicates with patients via a number of technologies, including cell phones; televisions, computers, or other home displays; or specially-designed alarm clocks or watches.

Greenberg gets reminders through his cell phone, but left the phone at home, he says. "Part of the point of vacation is to get away from your regular life. That means leaving things like cell phones behind."

Healthwatch officials point to a clause in Mr. Greenberg's policy stating that "failure to follow prescribed medical regimens, or to provide properly-formatted information documenting said regimens, will be cause for termination of coverage at the discretion of Company."

The information gathered on patient behavior possesses considerable economic value, and is leased to pharmaceutical companies and assisted-living technology developers, among others.

Mr. Kim, Mr. Greenberg's lawyer, argues that his client's case presents two issues.

"You've got the problem that a health insurance company is gathering incredibly detailed information on specific behaviors. This borders on the intrusive and Orwellian. Second, there are millions of elderly people and people managing chronic illnesses who are being offered systems like this. If insurance policies don't change, Mr. Greenberg's case will be just the tip of a very big iceberg."

Ironically, according to technology watchers, the problem may not be that systems like Healthwatch are too intrusive, but that they don't gather enough information to get a complete picture of a patient's behavior.

"Insurance companies were sold the idea of being able to see precisely what their customers are doing," says Jeffery Axelrod, a medical anthropologist at UC-Irvine exploring the intersection of "pervasive computing" and medical care. "But their systems are incredibly limited. People don't stand in front of their medicine chests waiting to take their medicines. They weave medical care into their lives, and take medicines everywhere—at work, at restaurants, while traveling. If insurance companies want to ding people for bad behavior, they need to be able to actually know how people are behaving."

The problem is exacerbated by the fact that different insurance companies use different data standards, making the construction of unified patient observation systems challenging. "These problems won't go away until insurance companies adopt a common standard for exchanging medical data," Lisa Bonnier, a medical informatics specialist, said. Varying state laws regarding information privacy have also added to the challenge. Washington and Colorado, where Mr. Greenberg lives and vacations, have conflicting regulations.

Paul Saffo, a director at the Institute for the Future, a Silicon Valley think-tank, said, "The paradox is that with today's health management systems, pervasive computing hasn't been pervasive enough."

Dr. Axelrod adds, "We all worry about electronic surveillance, but it may be that that the only thing worse than a system that can monitor your every move is one that can only monitor a few, but thinks it sees everything."

While Mr. Kim works on legal challenges to Healthwatch's decision, Mr. Greenberg is scrambling to find a new insurer. "I liked the system," he said. "It seemed to offer a reasonable tradeoff for me, But do I want another company to track this kind of information about me, and do a poor job of it? I don't know."

ABOUT THE ...

THE TECHNOLOGY HORIZONS PROGRAM

The Technology Horizons Program combines a deep understanding of technology and societal forces to identify and evaluate discontinuities and innovations in the next three to ten years. We help organizations develop insights and strategic tools to better position themselves for the future.

INSTITUTE FOR THE FUTURE

The Institute for the Future is an independent, nonprofit strategic research group with 35 years of forecasting experience. The core of our work is identifying emerging trends and discontinuities that will transform global society and the global marketplace. We provide our members with insights into business strategy, design process, innovation, and social dilemmas. Our research generates the foresight needed to create insights about the future that lead to action. Our research spans a broad territory of deeply transformative trends, from health and health care to technology, the workplace, and human identify. The Institute for the Future is based in Palo Alto, California.

ACKNOWLEDGMENTS

Author: Alex Soojung-Kim Pang

Artifacts: Jason Tester

Editor: Maureen Davis

Art Direction: Jean Hagan

Graphic Design: Karin Lubeck

124 University Avenue, 2nd Floor, Palo Alto, CA 94301 | 650.854.6322 www.iftf.org