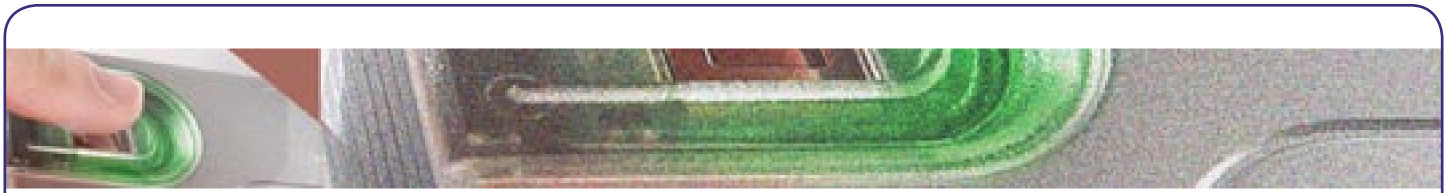


PUBLIC CONCERNS AND THE NEAR FUTURE OF RFID

What *really* worries people about RFID? This memo, *Public Concerns and the Near Future of RFID* (SR-926B, the second in the Technology Horizons series, *The Futures of RFID*), explores this question. Public worries about RFID fall into three areas: loss of privacy, loss of control, and the invisibility of the technology. This memo probes each of those concerns, and their sources.

Some concerns over RFID can be eased through better public understanding of what the technology is, and how it can be used or abused. But the best way to make RFID acceptable is not to have better PR, but better technology. Giving ordinary users more control over RFID—by giving them ability to remove or disable tags, or rewrite them—will eliminate many concerns about the technology. RFID is still malleable enough to be positively influenced by user concerns, public policies, and other externalities. If it isn't, it will face either legal restrictions and mandates, or user distrust and resistance. Smart privacy policies and design standards can work together to assure users that RFID will be designed and used in ways that they will find acceptable.

INSTITUTE FOR THE FUTURE

THE FUTURES OF RFID: A MEMO SERIES
Technology Horizons Program
June 2005 | SR-926B
www.iftf.org

The Futures Of RFID: A Series of Memos

To help **Technology Horizons Program** members understand the long-term potential 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. In 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. The third, **Flashpoints and Controversies** (SR-926C), 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.

THREE AREAS OF CONCERN

The impact of RFID on privacy is the best-known concern, and the most complex. According to some critics, the widespread deployment of RFID tags will lead irresistibly to surveillance and data gathering. In surveys and public discussion, many people treat privacy as an absolute. But in real life, privacy competes with other values: we regularly trade personal information for other things that we want, or exchange it to build relationships with other people. At both the personal and cultural levels, the boundaries of privacy change constantly; they are not absolutes.

People also worry about *control* over RFID. This is less often articulated as a worry, but it is at the heart of many frightening scenarios involving RFID. People worry about an inability to know whether tags have been disabled and whether or not they are being tracked. They also worry that RFID tags could be accessed or abused by unknown parties.

Finally, the *invisibility* of RFID is a double-edged sword. It adds to the technology's convenience and utility, but also feeds fears about its abuse. The small size of tags, and their potential to be woven into or embedded in other products, raises worries that owners could carry tags without their knowledge.

PRIVACY

Privacy concerns about RFID reduce largely to concerns about two related things: surveillance and data gathering. While these are two separate functions, among citizens and privacy advocates concerned about RFID they are often collapsed together, and will be considered together here.

Surveillance consists of real-time tracking of individuals: for example, using video cameras equipped with face recognition software to identify visitors to a sports arena. Data gathering consists of the preservation of information gathered by surveillance and other means: building databases with records of individuals' purchases, credit histories, and personal information, for example.

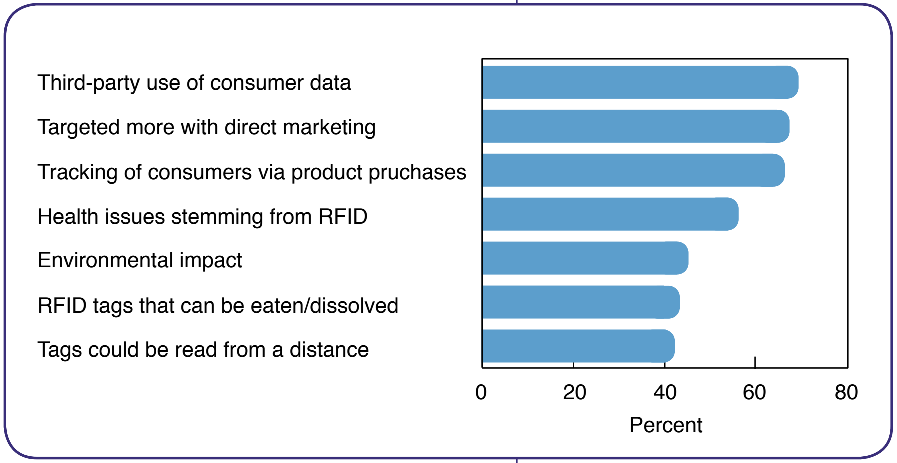
A special challenge is that, among privacy advocates, RFID seems useful for both purposes. Collections of RFID tags, one scenario holds, can be used to identify individuals by correlating particular items with their owners, either by matching ID numbers to owners, or by deduction (e.g., noting when and where items were bought). While this information could be used to identify individuals in real time, it could also be easily stored, and used to create detailed records of individuals.

A parallel concern is that, having been gathered, such data may exist for years. This violates a subtle but significant form of privacy, which legal theorists describe as "privacy from one's past." The basic notion is that we are held accountable for our actions and statements for some time, but not forever, and not in all contexts. Some serious actions, like violent crimes, may define a person for life. But we come to expect that lesser offenses or flaws—adolescent immaturities, political remarks in a late-night bar conversation, or accusations made in the heat of anger—are best forgiven and forgotten. One of the dangers that data gathering presents—and indeed all forms of computer memory—is that such events won't ever be forgotten, and individuals will lose the ability to grow beyond their own pasts.

Finally, among privacy advocates there is also the conviction that the mere storage of information invites mischief. Some critics of DARPA's Total Information Awareness program, the USA-PATRIOT Act, and other post-9/11 measures have argued that they hold great potential for abuse because they involve large-scale data-gathering programs. This has affected perceptions of RFID: as one privacy advocate put it, "The very existence of the database [of RFID consumer information] itself represents a threat to privacy, even if no one's using it today."

However, it is notable that a recent Cap Gemini Ernst & Young (CGE&Y) survey found that fears of active surveillance were not as great as worries about misuse of RFID-related data by third parties, direct marketing, and environmental concerns (see Figure 1).

Figure 1
Consumer Concerns Related to RFID
Percent of respondents who are "extremely concerned" about ...)



Source: Cap Gemini Ernst & Young, *RFID and Consumers: Understanding Their Mindset*, CGEY Executive Summary, 2004

2 Public Concerns and the Near Future of RFID

The Balance of Privacy

However, while it is common to think of privacy as sacrosanct and absolute, in reality it is not. That does not mean that it does not exist, or that companies need not respect it. Rather, it means that it is essential to understand the rules that determine when privacy can be given up, and what value one should expect in return.

Privacy Exists in Competition with Other Values

Privacy is valuable, but people are accustomed to trading degrees of privacy for other things that they value.

In the marketplace and public sphere, we often trade privacy for access to services, goods, or conveniences. Airport security measures require individuals to identify themselves, surrendering anonymity in exchange for heightened safety. Property rights require an owner to declare his or her identity: copyright and patent holders, for example, must reveal themselves to enjoy legal protections.

Private information is also regularly traded or sold for services and conveniences. Store club cards provide members with discounts or services, while giving stores the ability to collect information about members' buying habits. Credit card companies collect large quantities of data about users, but card holders are generally sanguine about such programs, since this information can be used for their benefit—to detect when cards have been stolen, for example, or to generate annual spending reports.

Utilitarian trades are also common in the digital world. Spam and virus filters, for example, work by reading a user's incoming e-mail. This is a form of "surveillance," but it also protects users from attacks and inconvenience. Recommendation systems like Amazon's operate by aggregating the preferences of millions of buyers, and delivering value back to individual shoppers in the form of purchase suggestions.

The highest-value exchanges are informal and result in the creation of new social goods. Indeed, the importance or relationships can be measured by the degree to which privacy barriers between parties are lowered. Individuals share secrets with one another to create or deepen friendships. Spouses trade physical and financial privacy (among other kinds) for intimacy, and to make it possible to share new duties or challenges like childrearing. Likewise, many professional relationships—between physicians and patients, lawyers and clients—recognize that privacy must be surrendered for effective service. Even in other services, privacy trades are the norm. Waiters at a favorite restaurant who remember your wine preferences, or a tailor who remembers what suits you've bought, possess uniquely identifiable knowledge about you.

But in all these cases, parties have rules that build privacy and trust around these relationships. They can be implicit (as between friends), or explicit (as with patient confidentiality or attorney–client privilege). More broadly, as communitarian philosopher Amitai Etzioni argues, to one degree or another, all social institutions provide benefits to their members at the expense of individual privacy, but also limit the extent of those trades.

For RFID and connective technologies, it's particularly important to note the opposition between privacy on one hand, and community and sociability on the other. Connective technologies are most attractive when they work as tools to bind people together, to create groups from individuals. Users will find services and technologies that use RFID to connect them to other people much more compelling than straightforward trades of privacy for cash. A world in which services that use RFID are overwhelmingly trade-oriented rather than socially oriented will be one in which acceptance of RFID is lower than it could be.

The Bounds of Privacy Alter over Time

One of the best-know projects in cultural history of the last two decades is the four-volume *History of Private Life.* Privacy, it turns out, has a history. It changes. And new technologies often play a role in facilitating and influencing those changes.

Indeed, it seems that new media always redraw the boundaries of privacy. Remember that the classic article 1890 by Louis Brandeis and Samuel Warren that established the concept of a "right to privacy" was inspired partly by the belief that urban newspapers were reducing privacy. Just as newspapers recast the boundaries between public and private life a century ago, today new media are encouraging individuals to recast the boundaries between public and private life. Technologies like blogs, instant messaging (IM), and Web cams are all used to project identity, build community, and maintain friendships.

2 Public Concerns and the Near Future of RFID

From Privacy to Publicity: The Case of Blogging

The blogging phenomenon shows how people renegotiate the boundaries between technology, privacy, and sociability—and how people are willing to reveal personal information for sociability, as long as they remain in control of the process.

Blogs began as online journals or notebooks. Today, they can include automatically generated information about an author's location; their accessibility via e-mail or IM; what online content they've recently read; and what books they're reading or music they're listening to. Blogs have evolved from diaries into identity-projecting media, broadcasting information about the author on a variety of channels.

Of course, blog authors must constantly think about what information to display, and what to keep private. Further, without exception, services that automatically post information about an author are opt-in. Not only do users have to sign up for them, they must also code their Web pages to display it. It is impossible to accidentally use one of these services.

The basic lesson we learn from the proliferation of blogs and identity-projection tools within blogs is clear. If given the option, some people will choose to display a remarkable variety of information about themselves, for the purpose of enhancing their reputation and attracting friends.

CONTROL

Indeed, it's more accurate to say that the big issue is not privacy as an absolute condition to be maintained at all times (no human lives this way), but control over the technology and its uses.

People are unsettled by technologies that they feel they can't control, or that have uncertain motives. They want to remain in control of their technologies. Computer users react poorly to software that is unpredictable. They actively dislike technologies like spyware because they are unpredictable and working for someone else. But they embrace some technologies that require they surrender privacy—if it is for a good purpose. For example, I have a piece of software that reads and analyzes every single piece of e-mail I receive before I see it. It's called my spam filter. Another piece of software monitors everything that I download or send over the Internet. It's called my antivirus program.

The number of technologies that are outside users' control is growing, as is public awareness of them. Indeed, a recent Pew Internet study indicates that a growing number of people are avoiding the Internet, or venture only to known and trusted sites, to avoid spyware and cookies that track their online activities.

In the case of RFID, control concerns reduce to two questions:

- What is it saying about me? Anti-RFID advocates have painted scenarios in which users have no ability to know what is on a tag, or whether it is alive or dead. They argue that users can never be sure whether tags have really been disabled, have been disabled but turned back on, or have been rewritten by unscrupulous retailers or other parties.

- Who else can access it? In anti-RFID scenarios, retailers, market researchers, government agencies, terrorists, or anyone else with the appropriate technology can read unsecured tags.

INVISIBILITY

Finally, the small size and intimacy of RFID contributes to a visceral sense that it is different from technologies like surveillance cameras or smart cards. Unlike bar codes or magnetic strips, RFID tags can be embedded in products, raising the specter of their being hidden from an owner's view.

What also sets RFID apart is its potential intimacy. A technology that you carry or wear is different from one that you pass on the street, or even have installed in your computer or car. Likewise, uncertainty surrounds the degree to which readers need to be visible. This explains why the most elaborate and dystopian scenarios spun by anti-RFID forces almost always include tracking of individuals using, for example, tags hidden in shoes and tracked by readers concealed under carpeting.

It's notable that RFID is entering public consciousness at the same time as nanotechnology, another heavily publicized and controversial technology whose invisibility is both a virtue and threat. Nanotechnology critics argue that the technology is fundamentally uncontrollable, and that users will never be assured that they're not being exposed to harmful nanotechnologies. The scale of the technologies is different, as are the specific worries (privacy and surveillance in the case of RFID, medical impacts or the rise of "grey goo" with nanotechnology); but the fact that both are the subject of public discussion may contribute to a collective sense of technology becoming ever more invasive and difficult to control.

THE MOST LIKELY NEAR-FUTURE USES OF RFID: SECURITY AND HEALTH

Ordinary people are most likely to encounter, and sometimes directly interact with, RFID in security and health applications. In the near future, most of these applications are not likely to raise privacy or surveillance concerns.

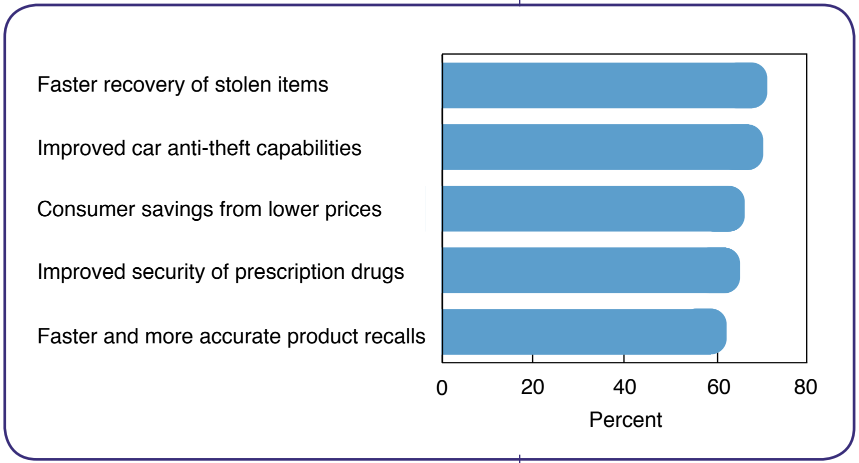
Security

RFID will be used in a number of security contexts. This is hardly surprising, given that CGEY's recent survey found that security applications topped respondents' list of the most attractive uses of RFID (see Figure 2).

One of the most important will be protecting the food supply. Tags are already being used in food safety and tracing systems in Japan, and are likely to become more popular in the United States. In Japan, RFID already reaches from field to store to restaurant. Fishermen in Miyagi prefecture use RFID tags as an authentication tool: customers use the tags to verify that shellfish deliveries are fresh and harvested legally. Supermarkets use RFID and sensors to check whether deliveries have been subjected to unusual heat or cold. A few restaurants use RFID-embedded plates to verify the freshness of prepared sushi.

More broadly, the Japanese government is pushing a three-year initiative to improve food traceability and make that information available to shoppers and diners. Services already exist that give users the ability to photograph a product's 2D barcode with their camera cell phones, and receive information about that product's history; as RFID readers become standard on cell phones, the food industry is likely to move from bar codes to RFID. Similar efforts will emerge in the United States. In the wake of the recent mad cow disease scare, plans are underway to tag cattle with RFID to make it easier to trace them through their lives and isolate diseased cattle.

Figure 2
Importance of Potential Benefits from RFID
(Percent of respondents who said ... is an "extrememly important" use for RFID)



Source: Cap Gemini Ernst & Young, *RFID and Consumers: Understanding their Mindset*, CGEY Executive Summary, 2004

Another area where people will see RFID is in aircraft baggage tagging. Currently, only bags going between specific points—Manchester and Frankfurt, JFK and Narita, Atlanta and Jacksonville, and a few others—are tagged with RFID, but the odds are good that in the next two years these systems will be adopted in other major airports, both as a safety measure and to increase the efficiency of baggage handling.

We'll also see some use of RFID to track people or objects in restricted areas. Prisons are experimenting with RFID-enabled handcuffs or clothes. A few amusement parks, most notably the LEGOLAND parks, offer tracking wristbands that can help parents locate lost children. Casinos in Europe and the United States are quietly introducing RFID-embedded chips to prevent counterfeiting, recover quickly after accidents (fights that overturn a table, for example), and to follow the behavior of users.

We're also seeing some services in which people add their own RFID tags to valuable items. Pet chips, embedded RFID chips that allow veterinarians to identify a pet's owners, are already common. Snagg (www.snagg.com/) is a service that allows owners of musical instruments to tag their instruments and register them in a database. About one million musical instruments, ranging from expensive violins to high school trombones, are stolen each year in the United States, boosting the need for instrument identification. Such systems are likely to expand, as consumers adopt RFID as a method of identifying and recovering expensive or otherwise precious goods.

Health

A second area where people will interact with RFID will be health. Once again, EPC (electronic product code) adoption in hospitals and other health care spaces will introduce users to the notion of EPC providing benefits that will eventually move into the home.

RFID is being used in a small number of hospitals in the United States and Asia to manage equipment, and to identify and locate patients. During the SARS epidemic in 2003, hospitals in Singapore and Hong Kong gave RFID-enabled ID bracelets to contagious patients and placed readers around quarantine wards. Such bracelets are now being adopted in some children's hospitals in the United States, to help match mothers and newborns.

RFID tagging is also being adopted for drug safety. Counterfeiting and theft are big problems in the prescription drug industry. Some $30 billion of counterfeit prescription drugs are sold every year, and inventory worth another $40 billion is lost or stolen along the pharmaceutical supply chain every year. The pharmaceutical black market rivals the narcotics trade in profitability, and deadliness. In response, Congress' Prescription Drug Marketing Act, and several state-level bills, require prescription medicines come with "pedigrees" to reduce counterfeiting. Paper pedigrees are difficult to manage; RFID tags offer the possibility of putting the pedigree directly on the packaging. The recently concluded Project Jumpstart demonstrated the viability of using RFID instead of paper to combat both problems. The tags serve as proof that a drug is what it claims to be, and its unique ID number can be used to retrieve information about its manufacturing, history, and expiration date.

Broader use of RFID to secure the pharmaceutical supply chain—at least for very popular drugs like Viagra and Lipitor—will happen in the next two to three years, according to an Accenture estimate.

RFID as an Additional Layer of Security and Traceability

In almost all these applications, RFID tagging will be fairly unproblematic, as it will layer atop existing security or traceability systems. RFID tagging of airline baggage, for example, is an incremental rather than revolutionary application. Bags have been tagged for decades, and since travelers already consent to having bags tagged and searched, using RFID won't raise new privacy concerns. Services like Snagg offer a modest tradeoff between security and privacy, but one that doesn't force owners out of established comfort zones: anyone who's registered a valuable product, or had a diamond etched with an ID number, will have already made such a tradeoff.

Institute for the Future, "Artifact from the Future"

Likewise, casinos, amusement parks, and airports are public spaces where you already voluntarily surrender a degree of privacy in exchange for security or entertainment. In the case of hospital applications, patients have an obvious interest in having doctors know where they are.

CONTROVERSIAL USES OF RFID

Other application areas hold the potential to generate controversy around RFID, or opposition to further deployment of the technology. In the third memo in this series, *Possible Flashpoints* (SR-926C) we will look at some of them.

Global deployment of RFID would be slowed if China developed its own, incompatible RFID standard.

Institute for the Future, "Artifact from the Future"

ACKNOWLEDGMENTS

Author: Alex Soojung-Kim Pang

Artifacts: Jason Tester

Editor: Maureen Davis

Art Direction: Jean Hagan

Graphic Design: Alexandra Weil

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.

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