RFID: IMPLICATIONS AND RECOMMENDATIONS

In the next decade, RFID will move from the supply chain into the world at large. In the near term—that is, over the next three to five years—the cost of tags and readers will fall enough to allow the technology to move onto products, clothes, and packaging. As it diffuses, RFID will appear in an ever-widening variety of social and use contexts. RFID will begin to be an element in hospital, airport, and store security; a tool to identify and recover stolen merchandise; and an instrument of contactless commerce.

Then what? Broadly speaking, there are two possibilities. RFID could become like genetically modified foods: a promising and much-hyped technology brought low by technical controversy, groups of activists, restrictive regulation, and confusion among consumers. Or it could explode beyond its early applications to become as ubiquitous as Internet routers, mobile phones, microchips, or bar codes: everywhere, uncontentious, their use and reuse easy and uncomplicated.

RFID is a technology whose future is still under construction. Steps taken now will determine the direction of its path.

What can companies do to encourage popular trust in RFID and avoid controversies? In the near term, it will be essential to build trust. Users and other stakeholders must trust not only the technology, but that the data generated by RFID will be stored and used responsibly. Finally, users will have to trust their own judgment about RFID. In the future, the most knowledgeable users will be the most enthusiastic.

No single strategy will deal with all these issues. It will be necessary to pursue several strategies simultaneously, changing focus over time as RFID evolves.

5 RFID: Implications and Recommendations

The Futures of RFID: A Series of Memos

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. The third, **Flashpoints and Controversies** (SR-926C), focuses on controversial potential uses of RFID. The fourth in the series, **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 this 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.

WHAT TO DO IN THE NEAR TERM

In the next several years, companies should focus on three things: educating users about RFID; developing design standards of RFID systems elements; and guiding the use of such elements in products to avoid potential problems. Companies should also develop general information and privacy policies that promote consumer trust.

Educate Users

Well-informed consumers make good technology users. They know when to reward companies with loyalty. They are more likely to adjust successfully to new technologies. And they reinvent and innovate their use of recently created products.

Today, most users and anti-RFID groups conflate concerns about the technology, database mining, and police surveillance. It is useful to distinguish privacy fears that are RFID-specific from those that concern all surveillance technologies (for example, video cameras and biometrics); from problems that result from the theft or misuse of databases and their mining; and from dangers of state surveillance.

Today, people are far more concerned about the misuse of data and targeted marketing (neither requires RFID) than they are about tracking. This suggests that a distinction can be made in the public mind between these technologies and activities. This distinction would allow companies to make common cause with privacy advocates. For example, in agreeing that inadequate protection of privacy data in government-issued IDs represents a greater concern than the readability of RFID tags in tires, companies and privacy advocates build a foundation for working together to refine technical and design standards, pushing RFID development in positive directions.

The scariest scenarios involving RFID are also the most unrealistic. For example, there is speculation that RFID will "create a world subject to total surveillance," destroy anonymity, and expose consumers to predatory marketers and techno-savvy criminals. These claims are only reasonable if you assume that FCC regulations on RF signal strength will be eliminated; corporations and governments will spend hundreds of billions of dollars installing RFID readers in public buildings, stores, and homes; and the price of tags will suddenly plummet. It's more reasonable to take seriously concerns about the appropriateness of using RFID in passports and the conditions under which retailers will disclose when they gather information about users' behavior. These more realistic concerns about RFID use will help discredit the more extreme scenarios and guide public discussion to more useful issues.

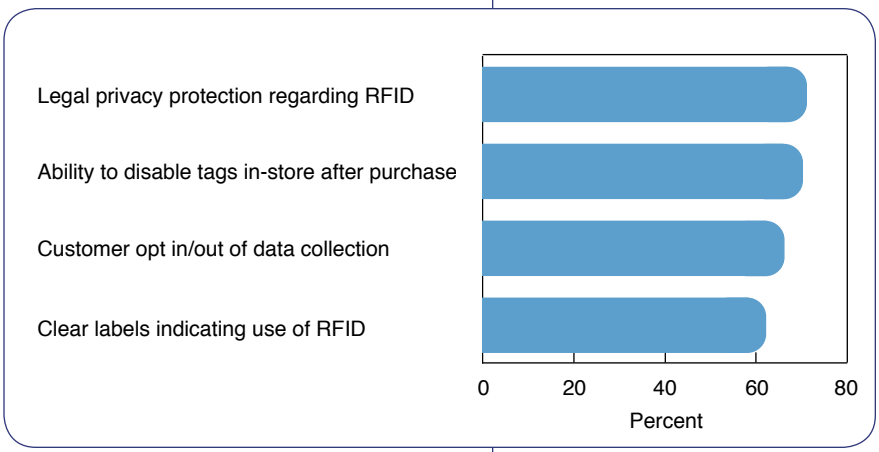
Develop Design Standards

Technologies reflect both the values of their creators and the demands of their users. Companies can develop design principles to highlight their commitment to end-user privacy and control and to meet public expectations.

Clues that may help direct the design of these principles can be found in a recent survey of consumer attitude toward RFID technology. As Cap Gemini Ernst & Young found, a majority of consumers said that they would be more willing to buy RFID-enabled products if they could disable tags, opt in or opt out of tag-based data collection, and if product labeling clearly identified which products were RFID-tagged (see Figure 1). These results confirm the recommendations of other groups who argue in favor of tag visibility, destruct capability, and voluntary participation in data-collection programs. More generally, the results suggest several design principles.

Consumer backlash to RFID will likely be avoided by educating consumers about the technology.

Figure 1
Factors Affecting Willingness to Buy RFID-Enabled Products
(Percent of respondents who would be more willing to buy RFID products)



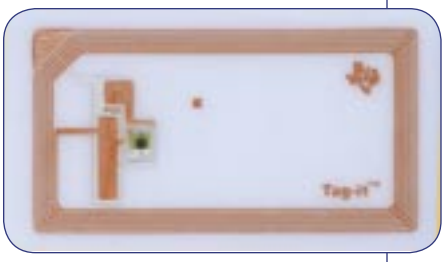
Source: Cap Gemini Ernst & Young, *RFID and Consumers: Understanding Their Mindset, CGEY Executive Summary*, 2004.

5 RFID: Implications and Recommendations

Highlight Control

Consumers should always know when a tag is in use on a product and should be given the means to disable or destroy the tag if they choose.

Having control over a technology is the first step in trusting it enough to extend its use. People need to believe that their devices are working for them, not secretly informing others (for example, insurance companies, HMOs, or police) about them. This is an especially sensitive issue for intimate products that people regularly carry or wear close to the body.



Most importantly, consumer goods should have tags that can either be removed or disabled after purchase. Consumers should have the power to permanently disable EPC tags themselves. This could be done by working a strip into the antenna that, if torn, disables the antenna; or fashioning a corner that users could fold to break the contact between tag and antenna, rendering the tag mute; or giving users the ability to completely remove the tag from a product. Manufacturers might encourage appliance companies to add an "EPC destruct" button on the microwave that would destroy the chips.

Make the RFID Tags and Their State Visible

Users should never be surprised when they see a tag on an item. Wherever possible the tag should be visible in the design of a product. Similarly, the product's owner should be able to see whether a tag is functional. If a consumer chooses to disable a tag, that should be reflected in the appearance of the tag, as well.

Calibrate Privacy Protections to the Value and Mobility of Goods

Consumers will welcome RFID technology to help them track and protect valuable items.

Different products will demand different levels of privacy protection and user control. Placing encrypted tags on a box of laundry detergent makes little sense. Detergent is relatively inexpensive and is used in unsurprising contexts (for example, laundry room, laundromat).

In contrast, users are more likely to demand encryption in clothing. Clothes are worn repeatedly and in a multitude of contexts. Many people think of clothes as tools of personal expression and identity projection. (As the saying goes, "clothes make the man.") Some users may want their clothes to broadcast those signals and make them digitally accessible. Bloggers have made it apparent how many people are willing to publicize details of their lives in exchange for enhanced sociability. But blogging is a voluntary activity; bloggers choose what to reveal and what to conceal. People will want to be able to make the same choice with tagged clothing.

On the other hand, users will want permanent, unalterable tags on valuable possessions. If a stereo system, leather sofa, personal safe, or other valuable leaves the home, the owner will want to know about it. So, consumers will want some tags to

be permanent—designed into products with read-only capabilities—in order to facilitate the identification and recovery of stolen items.

As a rule of thumb, products that stay in the home (for example, home-care products) or have short life spans (for example, personal-care products) won't require additional privacy protection. Products that travel, are worn, or have long life spans may deserve encryption. This follows standard practice with technologies. We routinely put more security (physical measures, like locks and protective cases; and risk mitigation technologies, like insurance) on valuable items than on cheap ones. A tricycle is outfitted with less security than a Lexus. Similarly, we expect a financial services company to have far better security systems in place than would a fast-food restaurant.

Promote Open Systems and Common Standards

In the short term, intelligent companies can benefit by being first to market with RFID-enabled products and working with partners to develop devices that empower users. Over the long-term, companies will derive greater benefit by creating an open system based on common standards and by encouraging retailers to open elements of their reader systems to customers.

No one makes money off standards. But everyone makes money because of standards. Common standards grow markets faster, allow third parties to build new products or services that draw upon existing goods, lower the costs of integration, and make consumer products easier to use.

Standards are as essential in the information technologies arena as common language is for human communication. The phenomenal growth of the World Wide Web in the 1990s owed a great deal to two key features: the Web was based on open, royalty-free standards, and its architecture was designed to allow anyone who conformed to those standards to develop new software and hardware. That openness has not stifled innovation and entrepreneurship. To the contrary, it has made Amazon and eBay possible. The proliferation of RFID in new markets and use contexts will undoubtedly push the envelope of existing standards. But the overall growth of RFID should be conducted within common standards frameworks as much as possible.

Not only should RFID systems conform to open standards, retailers should look for opportunities to help consumers by opening their own RFID infrastructures. For example, amusement park security company SafeTZone currently operates a "walled garden" of readers and tags. In a few years, it will make sense for SafeTZone to open the readers to parents who want to track their children using the child's RFID-tagged clothing—the parents would rent reader access rather than an entire RFID system. Likewise, retailers could open their RFID readers to help parents locate lost children in stores and malls.

5 RFID: Implications and Recommendations

Guide RFID Use to Avoid Problems

Educating consumers and adopting good design practices will help create a climate in which RFID can be intelligently deployed and used. Nevertheless, companies will also need to be mindful of what they shouldn't do with RFID. Here are a couple points to consider:

You Can Hide RFID, But It Won't Stay Hidden

RFID tags are cool because they're lightweight, unobtrusive, and they can be embedded in packaging and products. They're also bad because they're lightweight, unobtrusive, and they can be embedded in packaging and products. Under the wrong conditions, technical virtue can become social vice.

Unlike a bar code, which is always visible to enable its scanning, an RFID tag can be placed on the inside of a package or the underside of a product, entirely out of view. Strategic placement of tags helps protect them from everyday wear and tear. After all, the RFID tags are intended to have a longer life span than bar codes. In some circumstances, however, placing tags that are hard to find and not providing some indication that tags are on a product, may seem as though the device was purposely hidden—or that the product manufacturer has something to hide.

For a technology that's so small, RFID does a terrible job of being invisible. For the system to work, readers must talk to tags, and tags must answer back. In the near future, readers will be detectable by people carrying the RFID-equivalent of a Wi-Fi finder. (As the communication frequencies of tags become standardized in retail applications, readers will become easier to detect.) Anyone with a reader will be able to detect a tagged product or package within a matched frequency even if the actual data can't be read off the tag.

Smart companies will design RFID into products in ways that protect the tag but don't look sneaky. They'll conduct tests that aren't disruptive but also don't look secretive. This will be particularly important while the technology is still new and controversial and advocacy groups are mobilized to quickly spread the word about suspicious tests. Eventually, RFID's novelty will wear off; but for the next couple years, it should be considered a factor in consumer reactions.

It is better for RFID tests to start off public and transparent because they're probably going to end up that way.

Context Matters ... A Lot

In the near future, RFID will cause the fewest problems when it's perceived as a layer atop existing security or systems.

There are plenty of contexts in which we temporarily give up a measure of freedom or privacy in exchange for security. It will not be an unpleasant surprise to see RFID tags in airline baggage tags, for example. (There actually are several airports and airlines conducting trials with RFID-embedded baggage tags. Major airports could begin regular use of the technology within the next couple years.) Bags are already searched. People expect airlines and authorities to be proactive in defending them against threat. And paper tags have long been used to track luggage. Adding an RFID tag would be easy. If RFID can be used to better track air cargo—which is currently under-searched—then so much the better.

Likewise, casinos have been quietly rolling out new poker chips with RFID tags embedded. When you think about it, poker chips and RFID were destined to be together. Poker chips are small, yet very expensive. If you're a gambler, you want to keep track of every single one. If you're a casino operator, you want to make sure that every chip played is legit, not a counterfeit. Like airports, casinos are awash with surveillance and security.

The context in which RFID is deployed will matter. Consumers will accept the technology in places where it makes sense, like airline baggage tracking and poker chips in casinos.

5 RFID: Implications and Recommendations

OVER THE LONG TERM

Assuming no backlash, RFID technology will become cheaper, more powerful, and ubiquitous as the decade wears on. As that happens, companies will have to adjust their priorities, both to accommodate changes in the technology and to take advantage of new opportunities.

Promote User Reinvention and Innovation

User innovation works in open systems that users can explore and alter, but not damage. The Internet has been tremendously successful as an incubator of user innovation. This is because its underlying architecture is public knowledge, yet cannot be accidentally altered by the inexperienced. RFID systems that users can explore and extend will become breeding grounds for experimentation and innovation.

Manufacturers and retailers should not try to suppress users from sharing their product experiences with one another, even if that means allowing consumers access to negative reviews while they browse the supermarket aisles. A pervasive computing world is a world of pervasive communication and pervasive information. Transparency is credibility. Attempts to block information will be met with great suspicion.

As prices drop and people look past privacy concerns, consumers will find personal benefit in RFID. Customizable tags will allow users to tag their stuff and will spark innovative uses we can't even imagine today.

Companies can't drive user reinvention, but they can both support it and benefit from it. User reinvention, by definition, is something companies cannot anticipate. By supporting standards and industry practices that encourage user innovation, and by closely following emerging practices with an eye toward incorporating those innovations into new products, companies can both support user reinvention and benefit from it.

What does this mean for RFID? Most importantly, it means that companies should push toward rewriteable tags, which users can erase and reprogram for their own purpose.

Customize User Experiences to Context

The emergence of flexible displays and pervasive computing will make it possible to deliver real-time product information, in ways that better instruct consumers about how best to use the products. There is a world of difference between reading instructions on a package or in an accompanying booklet, and interacting with a package that provides novices a step-by-step video explanation and offers advanced users the finer points of a product's capabilities and benefits.

As Lewis Pinault writes in *The Play Zone*, this is a world in which "differentiators [between companies] become more service than price, setting the stage for ... new robust and stable patterns that put the consumer first." Companies that merge content and products will be "marketing solutions rather than discrete products, learning about their consumers through in-house consumption regimes and then supporting their lifestyles accordingly."

Follow User Needs and Innovation, not Products or People

It is always useful to have data on consumer product use. But the highest ground—that which offers the greatest reward—comes from following innovation and creativity, rather than ordinary behavior. In a pervasive-computing world, users will have ample opportunity to find new and interesting uses for products, adding value to them (through content or social networks), and extending their capabilities. Very little about RFID's novelty will come from the technology itself. Instead, it will arise from innovative use. When it comes to finding new ways to use RFID to create and build product value, user experimentation will benefit company interests.

Move from Transactions to Connectivity and Relationships

Transactions that trade personal information for time or cost savings have their place, but they are not likely to promote widespread consumer acceptance of RFID or its regular use. In contrast, home readers (and other technologies that allow consumers to use RFID for themselves) will provide a foundation for using RFID to build relationships rather than facilitate simple exchanges.

The sweet spot will be to use RFID in systems that bring people together, that help them find like-minded people in the real world, or that connect people who can help each other.

5 RFID: Implications and Recommendations

ACKNOWLEDGMENTS

Author: Alex Soojung-Kim Pang

Artifacts: Jason Tester

Editors: Maureen Davis and Kymberli Hemberger

Art Direction: Jean Hagan

Graphic Design: Robin Bogott and Karin Lubeck

ABOUT 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 identity. 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