Security Management ONLINE

A chip off the privacy block?(RFID)

CONCERNS OVER PRIVACY raised as a result of advancements in technology have joined religion and politics in the pantheon of discussion topics guaranteed to result in an argument, with deeply polarized advocates on both sides digging in to immovable, and often extreme, positions. While these arguments often taper off as the technologies become more commonplace and well-accepted--think of concerns once raised by now-common devices like cell phones and bar codes--it is inevitable that as technologies begin to be applied in new areas, the same concerns will arise.

One of the latest candidates for the technology-versus-privacy debate is radio frequency identification (RFID) tags. Proponents of the tags see these devices helping businesses to save millions by making supply chains more efficient and by reducing theft of high-value items. Detractors raise the specter of businesses tracking consumers without their knowledge or consent in a way that would not be possible with bar codes, which RFID tags are slowly replacing. Both sides raise important issues that need to be considered as use of RFID becomes more widespread.

RFID Basics

There are two basic types of RFID tags: passive and active. They differ in many ways, from their source of power to the distance at which they can be read.

Passive. Passive tags have no power source; rather, they are activated by energy emanating from a reader, and once activated can transmit a small amount of data to the reader. Because this method does not generate much power, the range at which passive tags can be read by a reader is small; experts say that 18 inches is about the maximum distance for typical passive tags to be regularly and correctly read without interference.

These tags are used on pallets and cases, and occasionally on items themselves, particularly high-value and frequently shoplifted goods (Gillette helped pioneer this field by attaching tags to packages of razors). They can also be found in commuter passes and access-control badges. Passive tags are inexpensive, costing less than a quarter, and most experts say that the price is likely to drop to about a nickel per tag.

Active. Active tags use a small power source such as a battery to transmit a continuous signal that can be picked up by a reader. They are more expensive (twenty dollars or more) and much more powerful than passive tags; they can be read from hundreds of feet away. These tags can be found in applications that require long-range read capability, such as EZ Pass automated toll collection cards or cargo transit systems.

This article focuses on passive technology because that is the type of tag being used in consumer goods and IDs, including company access cards and passports (see sidebar for more on passports). It is, therefore, the one consumers most likely would use and it is also the focus of most of the arguments about privacy.

Privacy

Privacy questions are raised by two related concerns: the possibility of RFID tags being read by unauthorized, rogue readers; and the potential for organizations to track the movements and purchasing habits of consumers.

Rogue readers. Imagine that an item you purchase at Wal-Mart contains an RFID tag that is used to help the store keep track of the item as it is brought from the supplier to the store's warehouse and from the warehouse to the store. You take the item out of the store and place it in the trunk of your car. Could someone track your purchases once you leave the store?

Not easily, says Allan Griebenow, president and CEO of Axcess International, which provides RFID tags for physical security and supply-chain management. Griebenow says many privacy concerns are the result of misconceptions about RFIDs.

For example, he points out that the limitations inherent in reading tags at a distance or through barriers like metal make it virtually impossible for someone to read tags on items that have been placed, say, in the trunk of a car. "This level of concern that has popped up is obviously founded in a lack of understanding, or a lack of intent to understand, what the real properties of RFID are," he says.

Tracking consumers. But what if you purchased an item in one store and then went to another store where there was an RFID reader looking for tags on that store's items? Could the reader get data from the first tag? Yes, if the first tag was located within range of the store's readers, says Dr. Ari Juels, principal research scientist manager with RSA Laboratories. He says this case is likely to exist. "We have to assume, for instance, that many shops as a deterrent to shoplifting will have RFID readers in door portals, so it seems natural that consumers will be subject to scanning as they enter or leave shops," he says.

Privacy advocates rank the tracking of consumers and their purchases from store to store as one of the greatest concerns. But the day that happens may be far off, for several reasons.

First, item-level tagging is still rare, says Juels. "It's unlikely that individual consumer items are going to be regularly tagged for some time," he says. "It will be another 10 years at least before RFID is cost effective as a wholesale replacement for bar codes."

Second, the passive tags used for inventory purposes typically hold nothing but a unique serial number; the number has meaning only to the backend database of the organization that is tracking the tagged inventory.

Tags do not hold personally identifiable information about a consumer. Therefore, RFID experts say, even if it were easy to "sniff" data from a tag, that data would be worthless to the thief.

What's more, Griebenow says, since the data desired by a thief is already in a database, there are easier ways to take it than by somehow compromising an RFID tag. "Looking at privacy related to a technology concern in a vacuum means nothing if it's not placed against other means by which that kind of data could be derived. In this case, the expense that it would take to first capture and steal that data from an RF signal and then process it into something that would be usable or harmful is dramatically higher than the other mechanisms for a human to steal that data through other sources," he says.

But some privacy advocates are concerned that even without access to a database, efforts will be made to derive more information from the movement of tags themselves. Libraries provide an interesting case study for these kinds of concerns.

Many libraries have begun to put RFID tags on each book in their stacks to make it easier for staff to keep inventory and to allow patrons a self-checkout option. Researchers from the University of California at Berkeley studied the possibility of privacy problems arising from this use of tags and concluded that "today's practices and standards fail to protect patron privacy, and vulnerabilities are present at all layers of the system."

The study showed, for example, how privacy could be compromised even if a static identifier were used and there were no access to a backend database. For example, the authors postulate that someone could use an RFID reader inside a library to create a "hotlist" of books that could be searched for at other venues.

They explain that "readers could be set up at security checkpoints in an airport, and individuals with hotlisted books set aside for special screening." If it sounds theoretical, remember that the FBI warned that the presence of almanacs might be one red flag to terrorist activity, they write.

Transparency. In retail, the time of item-level tagging may be further off than for libraries, but privacy advocates worry that the risks of tracking are real.

"If you talk about the use of information on tags that is being matched with consumers' information, there are definitely risks," says Cedric Laurent, director of the International Privacy Project with the Electronic Privacy Information Center (EPIC). "You can get information about the tag itself, even just a serial number you can match with consumer information" if that consumer uses a credit card to make a purchase.

But that already happens. If you buy a product using a credit card, personally identifiable information about you and data about your purchase is captured via the product's bar code and sent to the store's database; if you use a "loyalty card" that offers discounts, stores can easily track your purchases and even send you mail or e-mail tailored specifically to your likes. So why would RFID pose a greater, or even different, threat?

Laurent says one reason is that RFID provides less transparency than bar codes, because they can potentially be read surreptitiously, even from your shopping bag, as opposed to bar codes, which need to be scanned with a reader.

A study conducted by the information and privacy commissioner of Ontario, Canada, concluded that RFID differs from bar codes in other important ways. For example, the report points out that with bar codes, every bottle of Coke has the same bar-code number, while with RFID, "every individual Coke bottle could have a unique ID number that could be linked to the person buying it ..." The report also notes that because tags don't need direct line-of-sight to be read, they can be easily hidden, "sewn into the seams of clothes, sandwiched between layers of cardboard, molded into plastic or rubber, and integrated into consumer package design."

All this means that consumers may not have an easy way to control what information they hand over to a retailer, or even be aware that they are doing so, which is not the case when consumers voluntarily use a credit card and a loyalty card. Laurent concludes, therefore, that it is extremely important to have "rules that protect people whose data is being processed from having that information be abused. [It is] only by putting in place data protection principles that we can avoid the problem," he says.

Such principles would impose limitations on the collection and retention of data as well as redress situations when data has been taken without consent or used improperly, says Laurent.

Privacy policies. Privacy policies offer one means of helping reassure consumers that their data will not be ill-used. However, these policies are of limited value, some experts contend.

"It's all very well if I buy an item from Wal-Mart and Wal-Mart has a very stringent privacy policy," says Juels, "but as soon as I leave Wal-Mart I'm no longer subject to" that store's privacy policies. "The policy is only as good as the extent of its reach," he says.

"Moreover, abuses can take place even in the face of policy, and it's very easy for companies to steamroll over consumer rights or to get consumers to waive their rights" without them fully understanding what they've given up, says Juels.

Government Action

Concern over the possible privacy ramifications of RFID has prompted many state legislators to introduce legislation that would limit the use of the technology.

A New Mexico bill introduced last year would have required RFID tags in or on consumer items to be removed or disabled after the items had been purchased. It also mandated that businesses display a sign notifying consumers that the shop carries tagged items. The bill further mandated that each tagged item bear a label indicating that the item contained an RFID chip. In addition, it gave consumers the right to request any personal information gathered through these tags. The bill did not pass.

The New Hampshire Senate passed legislation in April that would establish labeling requirements for and some prohibitions on the use of tracking devices in that state. Kathleen Carroll, HID's newly appointed director of government relations, was sent to New Hampshire to explain that the bill was misguided. She suggested to Senator Joseph D. Kenney (R-Wakefield) that an amendment be added to force the state to study the technology before passing a law. In April, Kenney introduced, and the Senate passed, an amendment that would create a commission to study RFID, comprising representatives from a range of interested parties, from the Senate to the New Hampshire Grocers Association.

Other states have made similar efforts. Texas considered legislation requiring notification if RFID was used in schools (the bill died when the legislative session ended). California has been considering legislation that would place a three-year moratorium on use of RFID in driver's licenses, student ID cards, health cards, and library materials. The bill has been on hold since late last year.

These are but a few examples of the approaches being taken at the state level. These various legislative efforts raise concerns among proponents of RFID not only because they would create a hodgepodge of rules but also because they are sometimes overly broad or vaguely worded, potentially impeding the market and making compliance difficult and costly.

The Grocery Manufacturers Association, which opposed the New Hampshire bill, for example, noted in a letter to the state senate that "laws specifically regulating RFID could stifle development of the technology before its benefits are fully recognized" and "could blunt the potential benefits consumers could derive from the technology of industry opposition."

In another example, AeA (formerly the American Electronics Association) opposed the New Mexico bill on the grounds that the definitions in the bill were vague and would impose an undue burden. The group noted that the bill defined "radio frequency identification" as "identification by technologies that use radio waves or other means to identify consumer goods automatically." [Italics in original.] That definition, according to the letter AeA's attorney sent to the state senate, "is so broad it could include bar codes or anti-theft tags."

Homeland Security. The Department of Homeland Security has issued a draft report on the use of RFID for human identification, which will be reviewed, along with industry comments, at a June 7 meeting of the DHS Data Privacy and Integrity Advisory Committee. The report has already generated concern by defining RFID broadly to include technologies such as bar codes and magnetic stripes in addition to smart cards, and by weighing in against all RFID technologies "for applications involving human identification" due to what the report views as potential privacy and data-integrity risks that would come with the use of RFID.

The Smart Card Alliance, which objected to those points, also took issue with the report's assumption that identification necessarily includes tracking. "The vast majority of identity applications do not track individuals," the group notes.

Industry Response

Companies with a stake in RFID technology recognize the need to deal forth-rightly with privacy concerns. That has led to coordinated industry action aimed at addressing public privacy concerns about the technology and fending off further state efforts to regulate its use.

In September 2005, HID announced a set of privacy principles that it would adhere to in making RFID tags. The principles cite the need for self regulation, urge that any time personal data is stored on a chip that it be subject to review by its owner upon request, and recommend that consumers be "aware of and consent to" the use of RFID tags.

The principles also make clear that HID does "not intend for our products to be used for sharing any personally identifiable information, whether collected on or linked to the tag with other parties, unless there is the clear consent of the user." (The principles are on the HID Web site.

The privacy principles were announced by all companies in the ASSA ABLOY ITG Group, but for other companies the principles are optional. Carroll says that, even so, she believes they should be best practices for all industries. She makes it clear that any company that uses RFID needs to take the privacy principles to heart if it hopes to win, and keep, customer support. "My focus will be on encouraging industrywide adoption of privacy principles ... so that the ultimate consumer has a comfort level with the technology," she says.

Best practices. In May, the Center for Democracy & Technology (CDT), a privacy advocate, released its own set of RFID privacy best practices. Paula Bruening, staff counsel for the group, says, "RFID best practices draw from principles of fair information practices. We looked at the technology, at the applications, how we see them possibly evolving, and then tried to figure out where RFID raises privacy concerns and where it doesn't." As was the case with the HID principles, choice and notice were found to be the areas of most concern.

Forum. HID sponsored an RFID forum late last year in Sacramento, California. The objective was to help improve understanding about how the technology works. Attendees included California State Senator Joe Simitian, who has introduced technology-restricting legislation, as well as representatives from the state's technology and chief information offices.

Dan Greenwood, a lecturer at the Massachusetts Institute of Technology's (MIT's) Media Lab who attended the forum, notes that the problems of legislation were a major topic of discussion.

"The principle we talked about there was that you can quickly run into problems with not having articulated the technology exactly right," Greenwood says. He notes that in Utah several years ago, lawmakers crafted legislation that directly affected public-key infrastructure technologies. "Frankly, the market [for this technology] moved on very quickly, so [the law] became obsolete," he says. "So you run the risks of either chilling innovation by people who want to meet the requirements of the statute or having legislation that's obsolete when the market moves on."

European Model

Since legislation concerning technology is hard to craft, how can lawmakers ensure that they are involved in protecting consumer privacy from any abuses of technology?

Some experts contend that it's simply too early to consider legislation. "When you have a new technology, a lot of times you have to wait and see where you have demonstrated problems before you can meaningfully regulate them," Greenwood says. Lawmakers should only "regulate in response to demonstrated market failures or demonstrated problems."

But Bruening argues for a more proactive approach. "There is a school of thought about privacy legislation that we should focus on harm from a civil-liberties perspective," she says. "The question becomes, how do you define harm? There are those who would draw it very narrowly, to say it's about identity theft and fraud, but for civil liberties, I think it's something broader than that, and that the way to approach this instead is to focus on baseline legislation that cuts across all technologies." She adds that it's necessary to put guidance in place "so that when new technologies emerge, industry has guidance about how to proceed with respect to privacy."

Laurent points to the European Union Directive on Data Protection as an example of legislation that is not technology-specific; rather, it "regulates any type of automated processing of personal data" and so would apply to RFID as well. Laurent says that a survey he's conducted on privacy in more than 70 countries shows that the majority follows the EU model of data protection. HID's Carroll agrees that "the European Commission has taken a proactive approach to these concerns," one that she hopes HID can emulate.

This type of high-level guidance is important, Laurent says, because the surreptitious nature of RFID makes it difficult to spot abuses in the first place. He notes that corporations are already using data from RFID tags to monitor employees despite or without privacy policies.

He cites a study conducted last year by The RAND Corporation that examined policies and practices at six private-sector companies. It found that five of the companies collected personally identifiable information from employee's RFID cards, often to monitor employee behavior. Only one company had an explicit written policy governing the use of RFID in its facilities, and none of the companies told employees "that data collected with access cards are used for more than simply controlling locks."

The Need for Partnership

Despite the sometimes rancorous debate, the positions that manufacturers and privacy advocates espouse don't seem all that far apart. Those who make RFID products insist that they do not oppose privacy protections. "We firmly believe that security and privacy are not mutually exclusive," said HID CEO Denis Hebert when introducing the company's privacy principles last year. And privacy advocates maintain that they do not want to stifle technological innovation.

Nevertheless, EPIC's Laurent expressed surprise that the group had not been invited to the privacy forum conducted by HID; at the same time, CDT released its RFID best practices after long discussions that did not include any RFID manufacturers. Representatives on both sides expressed a willingness to work together in future events.

Griebenow is sure that the issues can be worked out. "I'm confident that the privacy issues surrounding RFID will be fully vetted more intelligently as we move down the road, and that those concerns will go by the wayside much more rapidly than people perceive today."

For now, as chip prices drop and the number of items tagged rises, the debate over privacy issues will continue to rage. That's as it should be, says Greenwood. "What's happening now is very healthy," he says. The debate is a necessary part of making sure that RFID achieves its promise without stomping on the legitimate privacy concerns being raised.