RFID TAG—YOU’RE IT

Tiny radio-frequency identification tags, long used for tracking supplies and inventory, are now appearing in a growing range of consumer items. A privacy activist argues that the devices pose new security risks to those who carry them, often unwittingly

By Katherine Albrecht

If you live in a state bordering Canada or Mexico, you may soon be given an opportunity to carry a very high tech item: a remotely readable driver’s license. Designed to identify U.S. citizens as they approach the nation’s borders, the cards are being promoted by the Department of Homeland Security as a way to save time and simplify border crossings. But if you care about your safety and privacy as much as convenience, you might want to think twice before signing up.

The new licenses come equipped with radio-frequency identification (RFID) tags that can be read right through a wallet, pocket or purse from as far away as 30 feet. Each tag incorporates a tiny microchip encoded with a unique identification number. As the bearer approaches a border station, radio energy broadcast by a reader device is picked up by an antenna connected to the chip, causing it to emit the ID number. By the time the license holder reaches the border agent, the number has already been fed into a Homeland Security database, and the traveler’s photograph and other details are displayed on the agent’s screen.

Although such “enhanced” driver’s licenses remain voluntary in the states that offer them, privacy and security experts are concerned that those who sign up for the cards are unaware of the risk: anyone with a readily available reader device—unscrupulous marketers, government agents, stalkers, thieves and just plain snoops—can also access the data on the licenses to remotely track people without their knowledge or consent. What is more, once the tag’s ID number is associated with an individual’s identity—for example, when the person carrying the license makes a credit-card transaction—the radio tag becomes a proxy for that individual. And the driver’s licenses are just the latest addition to a growing array of “tagged” items that consumers might be wearing or carrying around, such as transit and toll passes, office key cards, school IDs, “contactless” credit cards, clothing, phones and even groceries.

RFID tags have been likened to barcodes that broadcast their information, and the comparison is apt in the sense that the tiny devices have been used mainly for identifying parts and inventory, including cattle, as they make their way through supply chains. Instead of having to scan every individual item’s Universal Product Code (UPC), a warehouse worker can register the contents of an entire pallet of, say, paper towels by scanning the unique serial number encoded in the attached RFID tag. That number is associated in a central database with a detailed list of the pallet’s con-
AVERAGE CONSUMERS may not realize how many RFID tags they carry around. The devices are embedded in personal items and even some clothing.

tents. But people are not paper products. During the past decade a shift toward embedding chips in individual consumer goods and, now, official identity documents has created a new set of privacy and security problems precisely because RFID is such a powerful tracking technology. Very little security is built into the tags themselves, and existing laws offer people scant protection from being surreptitiously tracked and profiled while living an increasingly tagged life.

**Beyond Barcodes**
The first radio tags identified military aircraft as friend or foe during World War II, but it was not until the late 1980s that similar tags became the basis of electronic toll-collection systems, such as E-ZPass along the East Coast. And in 1999 corporations began considering the tags’ potential for tracking millions of individual objects. In that year Procter & Gamble and Gillette (which have since merged to become the world’s largest consumer-product manufacturing company) formed a consortium with Massachusetts Institute of Technology engineers, called the Auto-ID Center, to develop RFID tags that would be small, efficient and cheap enough to eventually replace the UPC barcode on everyday consumer products.

By 2003 the group had developed a working version of the technology and attracted investment from more than 100 companies and government agencies. The tags’ promoters promised the tiny chips would revolutionize inventory management and counterfeiting prevention [see “RFID: A Key to Automating Everything,” www.SciAm.com © 2008 SCIENTIFIC AMERICAN, INC.}

© 2008 SCIENTIFIC AMERICAN, INC.
by Roy Want; Scientific American, January 2004].

To kick-start government adoption of the technology, the General Services Administration (GSA), a federal bureau that manages purchasing for other government institutions, issued a memo in 2004 urging the heads of all federal agencies “to consider action that can be taken to advance the [RFID] industry.” Suddenly, virtually every agency, from the Social Security Administration to the Food and Drug Administration, began announcing RFID trials.

During the same period, similar initiatives were under way around the world. In 2003 the International Civil Aviation Organization (ICAO), a United Nations agency that sets global passport standards, endorsed the use of RFID tags in passports. ICAO now calls for their use in all scannable “e-passports.” Today dozens of countries, including the U.S., issue e-passports with RFID tags embedded in their covers.

Since their debut, the new passports have been controversial on both privacy and security grounds. In a 2006 report one ICAO official promised that encryption measures would provide a “level of protection [that] should reassure the most anxious passport holder that his personal data cannot be read without his knowledge.”

Security experts quickly proved otherwise. In 2007 British security consultant Adam Laurie cracked the encryption code on a U.K. passport and “skimmed,” or remotely read, its personal information. And in what industry observers called the single largest RFID project in the world, the Chinese government is spending $6 billion to roll out RFID-based national passports for nearly one billion citizens and residents.

There is an important difference, however, between other nations’ RFID-based ID cards and Homeland Security’s new driver’s licenses. Most countries’ contactless national IDs and e-passports have adopted an RFID tag that meets an industry standard known as ISO 14443, which was developed specifically for identification and payment cards and has a degree of security and privacy protection built in. In contrast, U.S. border cards use an RFID standard known as EPCglobal Gen 2, a technology that was designed to track products in warehouses, where the goal is not security but maximum ease of readability.

Whereas the ISO 14443 standard includes rudimentary encryption and requires tags to be close to a scanner to be read (a distance measured in inches rather than feet), Gen 2 tags typically have no encryption and only minimal data safeguards. To skim the data from an encrypted ISO 14443 chip, you have to crack the encryption code, but no special skills are required to skim a Gen 2 tag; all you need is any Gen 2 reader. Such readers can be purchased readily and are in common use in warehouses worldwide. A hacker or criminal armed with one could skim a border card through a purse, across a room, even through a wall.

As of this past April, more than 35,000 Wash-
Living a Tagged Life

If the idea that corporations might want to use RFID tags to spy on individuals sounds far-fetched, it is worth considering an IBM patent filed in 2001 and granted in 2006. The patent describes exactly how the cards can be used for tracking and profiling even if access to official databases is unavailable or strictly limited. Entitled “Identification and Tracking of Persons Using RFID-Tagged Items in Store Environments,” it chillingly details RFID’s potential for surveillance in a world where networked RFID readers called “person tracking units” would be incorporated virtually everywhere people go—in “shopping malls, airports, train stations, bus stations, elevators, trains, airplanes, restrooms, sports arenas, libraries, theaters, [and] museums”—to closely monitor people’s movements.

According to the patent, here is how it would work in a retail environment: an “RFID tag scanner located [in the desired tracking loca-

The patent, here is how it would work in a retail environment: an “RFID tag scanner located [in the desired tracking locations] ... scans the RFID tags on [a] person.... As that person moves around the store, different RFID tag scanners throughout the store can pick up radio signals from the RFID tags carried on that person and the movement of that person is tracked based on these detections.... The person tracking unit may keep records of different locations where the person has visited, as well as the visitation times.”

The fact that no personal data are stored in the RFID tag does not present a problem, IBM explains, because “the personal information will be obtained when the person uses his or her credit card, bank card, shopper card or the like.” The link between the unique RFID number of the tag and a person’s identity needs to be made only once for the card to serve as a proxy for the person thereafter. Although IBM envisioned tracking people via miniature tags in consumer goods, with today’s RFID border cards there is no need to wait for such individual product tags to become widespread. Washington’s new driver’s licenses would be ideally suited to the in-store tracking application, because they can already be read by Gen 2 inventory scanners in use.

VOLUNTARY GUIDELINES

EPCglobal, Inc., an organization that sets standards for RFID tags, also offers principles for their use as “electronic product codes” in consumer goods.

Notice: “Consumers will be given clear notice of the presence of EPC on products or their packaging ... through the use of an EPC logo or [other] identifier.”

Choice: “Consumers will be informed of the choices ... to remove or disable EPC tags from the products they acquire.”

Education: Companies using EPC tags will “familiarize consumers with the EPC logo and help [them] understand the technology.”

Records: Consumer data associated with tags “will be collected, used, maintained, stored and protected by EPCglobal member companies in compliance with applicable laws.”

Types of Tags

Technical standards set by EPCglobal enable RFID tags to be grouped according to minimum capabilities. Each class adds to features of the basic class 1 tag, which is “passive”: it depends on a reader to initiate communication and supply power. Passive tags can be read from as far away as 30 feet, active tags from 300 feet or more.
today at stores such as Wal-Mart, Dillard’s and American Apparel.

A tracking infrastructure will become increasingly fruitful to marketers as more people begin carrying, and even wearing, RFID-tagged items. At present, tens of millions of contactless credit and ATM cards containing RFID tags are in circulation, along with millions of employee access badges. RFID-based public-transit passes, widely used in Europe and Japan, are also coming to U.S. cities. IBM’s person tracking unit is still only a patent, but an English amusement park called Alton Towers provides a living illustration of RFID’s tracking potential. On entering the park, each visitor is offered an RFID wristband encoded with a unique ID number. As people enjoy the attractions, a network of RFID readers placed strategically throughout the park detects each wristband as it comes within range and triggers nearby video cameras. Candid footage of each individual is stored in a file labeled with the wristband ID number, then made available to the customer on a keepsake DVD at the end of the day.

Protecting the Public

If RFID tags can enable an amusement park to capture detailed, personalized videos of thousands of people a day, imagine what a determined government could do—not to mention marketers or criminals. That is why my colleagues in the privacy community and I have so firmly opposed the use of RFID in government-issued identity documents or individual consumer items. As far back as 2003, my organization, CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering)—along with the Privacy Rights Clearinghouse, the Electronic Privacy Information Center, the Electronic Frontier Foundation, the American Civil Liberties Union, and 40 other leading privacy and civil liberties advocates and organizations—recognized this threat and issued a position paper that condemned the tracking of human beings with RFID as inappropriate.

In response to these concerns, dozens of U.S. states have introduced RFID consumer-protection bills—which have all been either killed or gutted by heavy opposition from lobbyists for the RFID industry. When the New Hampshire Senate voted on a bill that would have imposed tough regulations on RFID in 2006, a last-minute floor amendment replaced it with a two-year study instead. (I was appointed by the governor to serve on the resulting commission.) That same year a California bill that would have prohibited the use of RFID in government-issued documents passed both houses of the legislature, only to be vetoed by Governor Arnold Schwarzenegger.

On the federal level, no high-profile consumer-protection bills related to RFID have been passed. Instead, in 2005, the Senate Republican High Tech Task Force praised RFID applications as “exciting new technologies” with “tremendous promise for our economy” and vowed to protect RFID from regulation or legislation.

[APPLICATIONS]

**Everyday RFID**

RFID tags are embedded in a growing number of items people use regularly. They provide conveniences to consumers.

- **Airport baggage tag**
- **Toll pass**
- **Key fob**
- **Enhanced license**
- **E-passport**

Travel may involve multiple RFID tags, including toll passes and key fobs readable from significant distances, e-passports, “enhanced” driver’s licenses and some airport baggage tags.

**Schools and public libraries incorporate tags in student IDs, library cards and books. In the District of Columbia a new RFID-tagged “One Card” will serve as a public school student ID, library card and public-transit pass.**

<table>
<thead>
<tr>
<th>Reader</th>
<th>Tagged book</th>
<th>Combination ID library card and transit pass</th>
</tr>
</thead>
</table>

**[THE AUTHOR]**

Katherine Albrecht holds a doctorate in education from Harvard University and is director of CASPIAN, a 15,000-member consumer privacy organization opposing retail surveillance. Since 2003 she has worked to expose and prevent unethical uses of RFID in products and in people. She regularly testifies before legislators and delivered a keynote address at a workshop on RFID and privacy held at the Massachusetts Institute of Technology. She has also co-authored two books describing how corporate and governmental uses of RFID could threaten individual privacy and security.

© 2008 SCIENTIFIC AMERICAN, INC.
sumers or help businesses manage inventory or security. Increasingly, they also offer opportunities for marketing.

In the European Union, regulators are at least examining the situation. The European Commission—the executive arm of the E.U.—has acknowledged the potential for serious privacy problems with RFID and opened a public comment period earlier this year. As of July, when this issue went to press, recommendations stemming from the public comments were set to be released later in the summer, but expectations for any consumer-privacy regulations were low. In a March 2007 speech, E.U. commissioner for information society and media Viviane Reding announced that the commission would not regulate RFID but instead would allow businesses to regulate themselves. “I am here to tell you that on RFID, there is not going to be a regulation,” she said. “My view is that we should underregulate rather than overregulate so that this sector can take off.”

Unfortunately, industry self-regulation has little force when it comes to protecting the public from RFID risks. EPCglobal, the industry body that now sets technical standards for RFID tags, also produced a set of guidelines for the use of the chips in retail. The organization’s recommendations require, among other things, notice to consumers whenever products contain RFID tags—for instance, in the form of a recognizable RFID logo. Yet when Checkpoint Systems, a member company of EPCglobal, designed RFID tags to be hidden in the soles of shoes—in clear violation of the organization’s own provisions—Mike Miranda, then president of EPCglobal, told me that since the guidelines were voluntary, there was nothing he or his organization could do about it.

The Washington State Department of Licensing reassures citizens that their personal information is safe because the RFID tag in an enhanced driver’s license “doesn’t have a power source” and “doesn’t contain any personal identifying information”—even though those facts have no bearing on whether the card can be used for tracking. For some people, a false sense of assurance provided by such official mollifications could be dangerous. The National Network to End Domestic Violence, a group that vocally opposes the use of RFID in identity documents and consumer products, has submitted legislative testimony describing how abusers could use the technology to stalk and monitor their victims.

Meanwhile the RFID train is barreling forward. Gigi Zenk, a spokesperson at Washington’s licensing agency, recently confirmed that there are 10,000 enhanced licenses “on the street now—that people are actually carrying.” That’s a lot of potential for abuse, and it will only grow. The state recently mustered a halfhearted response, passing a law that designates the unauthorized reading of a tag “for the purpose of fraud, identity theft, or for any other illegal purpose” as a class C felony, subject to five years in prison and a $10,000 fine. Nowhere in the law does it say, however, that scanning for other purposes such as marketing—or perhaps “to control the population”—is prohibited. We ignore these risks at our peril.