

# Consumer Reports Looks at RFID

The consumer watchdog magazine examines the privacy and security concerns linked to the use of RFID in consumer products.

By Mary Catherine O'Connor

May 8, 2006—In its June 2006 issue, *Consumer Reports* rates laptops and PCs, considers the safety and comfort of bike helmets and lists the top gas grills for \$500 or less. It also provides its 4 million subscribers with a seven-page, in-depth look at RFID tags, which will likely one day be embedded in just about every product the magazine writes about.

"The purpose of the report was to explain what the technology is and what kinds of concerns need to be addressed," says Andrea Rock, *Consumer Reports* senior editor and the author of the article. The main concern, she explains, is that identity thieves might find a means of using RFID technology to aid in the unauthorized collection of personal information.

The article points out some advantages to be gained from the use of RFID technology. "Radio-tagging products from CDs to shampoos can offer huge cost savings to business, consumer conveniences such as speedier checkouts, and public benefits, including ways to manage toxic waste and encourage recycling," Rock writes in her report. But her primary focus is reflected in the article's title, "The End of Privacy?"

"Could a high-tech thief 'break into' the tags and cull your banking or medical information? And what about your privacy?" the article poses. Setting out to answer those questions, Rock interviewed industry associations, security experts, end users and RFID technology vendors. In so doing, she found that despite pending legislation and technological measures designed to address concerns over RFID being turned into a tool for surveillance or theft, the RFID industry has thus far done little to ensure consumer privacy.

The article does not prescribe who should be responsible for addressing privacy concerns. However, Jim Guest, president of Consumers Union—the company that publishes *Consumer Reports*—states in his June 2006 magazine column: "What we need is an array of strict and enforceable state and federal laws that safeguard consumers' privacy rights against all types of current and future gizmos. The laws should apply to any entity that collects and holds information. They should regulate, for example, the kinds of data collected, how the data can be used, consumer notification of security breaches and consumers' ability to see and correct their information. These rights should be enforceable by federal, state and local officials, and by consumers themselves."

The article maintains that by 2004, more than half of all U.S. companies were under mandates to implement RFID, a statistic Rock says was culled from a 2004 report written by consultancy Accenture. Despite that, she says, relatively few consumers even know what RFID is and how it is being used now—in applications many consumers enjoy, such as electronic toll collection—or could be used in the future.

RFID industry group EPCglobal has a list of guidelines for how the technology should be deployed in consumer items, and how its use should be communicated to consumers. Overall, Rock notes, the industry is

pushing for self-regulation and against the passage of any laws that would prescribe how the technology could or could not be deployed. In fact, the article quotes Jack Grasso, EPCglobal's senior director of corporate communications, as saying legislation is not needed at this time.

Still, that doesn't mean privacy concerns are being completely disregarded, according to Mark Roberti, editor and founder of *RFID Journal*, whom Rock also interviewed. "Corporations, even if they're self-interested, know that the way to make money generally is to do the right thing, so they won't alienate customers by violating their privacy," Roberti told Rock.

Last week, the Center for Democracy and Technology (CDT), a Washington, D.C., policy group, released a set of best practices as a means of establishing a baseline for companies using RFID to regulate how data linked to RFID tags is used, and how consumers should be educated about the technology (see Policy Group Spearheads RFID Best Practices). The best practices document is supported by a number of vendors of RFID technology, including IBM and VeriSign, as well as such end users as Visa USA.

Rock cites companies that have taken a proactive approach to protecting privacy while using RFID. "There was no public uproar," she writes, "when Marks & Spencer, a British retailer, used disposable RFID-tagged paper labels while testing the technology on men's apparel. Customers received brochures about RFID and the promise that the store would make no link between information on the tags and purchasers' identities, even if they paid with credit cards."

Still, Rock says she inadvertently collected evidence that in some cases, industry leaders are dodging privacy issues. She received an e-mail response to a request for an interview with Alien Technology, for instance, that mistakenly included a forwarded response from Linda Prosser, its vice president of corporate marketing. In that forwarded response, the article claims, Prosser suggested its outside PR firm make excuses to avoid contributing to the article if it would be "a privacy story."

This, Rock says, shows that some players in the RFID industry might consider privacy to be "more of an annoyance to be dismissed" than a real concern. Prosser, however, claims Alien was not dodging the privacy issue—rather, she says, her company suggested Rock speak with EPCglobal regarding the issue, which the article did not mention. "When we get inquiries from reporters who want to talk about privacy, we refer them to EPCglobal because we support EPCglobal's privacy guidelines. [EPCglobal] is the best group to address the issue of privacy," says Prosser. "We are the provider of the technology and not the user. A lot of issues around privacy are about the choices that the user makes, relative to privacy, so that user is a better source for that perspective."

Grasso further notes that although the quotes attributed to him in Rock's report are all accurate, the article is "fraught things that aren't true." For example, he says, "They start off by saying the technology will be used to collect info about you [consumers]. That's not true. This technology is about products and not people. It also talks about read ranges as much as 750 feet, but this is for active RFID technology and is not even remotely indicative of the overwhelmingly more common passive tags," which, he points out, have a read range of a matter of feet.

Grasso says the article also focuses on the use of RFID in pharmaceutical companies to save them money, but does not discuss the ways the technology could also be used to cut down on counterfeit drugs, thereby making them safer for consumers.

During the three months she spent investigating and writing the story, Rock states, news reports emerged about ways data encoded to some types of RFID tags can be surreptitiously collected or destroyed (see EPC Tags Subject to Phone Attacks). "As part of our coverage of new credit cards, such as Chase's blink card, we discovered that RFID technology was growing very fast," Rock says, "and we like to stay abreast of any new

technology than can impact consumer products."

In writing the article, Rock says she found that privacy concerns are not part of "a grand conspiracy," as some might think. "They [consumer privacy and security] do have to be addressed early on, and they deserve more than lip service."

EPCglobal says it respects the work that *Consumer Reports* does in attempting to educate consumers. Still, Grasso says, "If this was the only thing people read about RFID technology, they would be scared to death of it—and we don't think that serves consumers or businesses."

Copyright ©2005 RFID Journal, Inc. All Rights Reserved