

Instead of killing RFID tags to protect consumer privacy, we could add a privacy bit.

May 2, 2005—RFID privacy inflames passions as few other technological issues can. Readers of this journal are familiar with the enormous swirl of media attention around the topic. A statistic compiled by Ravi Pappu of ThingMagic summarizes the situation nicely: Of the Web pages returned by a Google search on the term "RFID" in late 2003, some 42 percent also contained the word "privacy." If item-level RFID tagging comes to pass, there is no gainsaying the privacy concerns it will bring. There is a real possibility of constellations of small wireless devices promiscuously emitting personal information. Some of the backlash against RFID, however, has assumed a form that is purely dramatic. Terms like "spy-chips," for example, neatly encapsulate the anxieties of a certain class of RFID opponent. But they distort any meaningful discussion of the uses of RFID, deny its benefits and cast privacy as a black-and-white issue.

The RFID community largely sees through extreme claims about privacy. What it overlooks is the dramatic nature of its own response. To address the problem of consumer privacy, RFID vendors and users have designed EPC tags of the Generation 2 variety so that they can be "killed." Killing means rendering tags permanently inoperative at the point of sale. This solution to the privacy problem—preemptive capital punishment for RFID tags, as it were—is psychologically gratifying; it is simple and direct. But it too casts the question of consumer privacy in black-and-white terms. The practice of killing RFID tags presupposes that their dangers to consumers are otherwise uncontrollable. The collateral damage would be extensive.



Killing tags would kill many visions of RFID benefit for consumers. If consumers possess only dead RFID tags, then smart appliances such as RFID-enhanced refrigerators, ovens and washing machines will be unrealizable. Likewise, RFID systems to aid the elderly with medication compliance and navigation of their environments will be more difficult to deploy. The killing of tags would preclude many other possibilities for consumers, like item returns in retail shops without receipts (not to mention the concomitant benefits to industry, like refined quality-control information), retrieval of lost items, automated product-part searches and so forth.

If RFID tags are killed, perhaps the greatest loss will be the innovations that have yet to be dreamed of. The Internet extended the reach of computing systems in ways that were unimaginable a decade or two ago. RFID will extend the Internet, and give rise to an infrastructure in which computing systems possess a new awareness of the world around them. Live RFID tags in the hands of consumers could open the sluices for another torrent of invention.

To construct a broad RFID infrastructure safely, a balance needs to be struck between privacy and utility. The benefits of tags must be readily available, but so too should the means for restricting their emission of information. The aim of this article is to describe the privacy bit, a simple technological tool

that helps achieve such a balance. The privacy bit may be viewed as a natural extension of an existing technology known as electronic article surveillance, or EAS. EAS can serve as a conceptual and technical bridge for the privacy bit.

Electronic article surveillance

EAS is commonplace and familiar to most consumers. Many articles in shops—from books to hair driers—bear small tags for theft prevention. At the point of sale, sales clerks deactivate these tags, generally by passing them over demagnetizing blocks. When a patron removes a tagged article without payment—or a sales clerk neglects to deactivate a tag properly—an alarm sounds at the shop exit.

EAS tags and RFID tags are similar in form. Inasmuch as they both track the whereabouts of objects, they are similar in function as well. The marriage of the two technologies is therefore natural, and some vendors are already integrating EAS functionality into their RFID tags (see [Checkpoint Bridges EAS-RFID Gap](#)). One way to implement EAS in an RFID system is to deactivate tags at the point of sale, as is done today.

An alternative is to set aside a logical bit on the RFID tag. This bit is initially off when items are in the shop. The bit is flipped to the on position to deactivate a tag at the point of sale. To allow purchased articles to pass without activating an alarm, the anti-theft gates at shop exits disregard tags whose bit is on. If live RFID tags and EAS systems are to coexist, bit flipping is the only viable approach.

Like an EAS tag, an on/off bit in an RFID tag can be informative: It indicates whether an item belongs to the shop or to a consumer. Theft prevention is therefore only one possible use for this bit. As we shall explain, this bit can also serve to protect consumers against unwanted RFID scanning. Indeed, this bit is what we shall refer to as the privacy bit.

The privacy bit

If RFID readers in shops refrain from scanning private tags, i.e., those tags whose privacy bit is turned on, then a good measure of consumer privacy will already be in place. Tags belonging to consumers in this case will be invisible to shops. At the same time, tags on items on shelves and storage rooms, i.e., those that have not yet been purchased, will be perfectly visible. The privacy bit will not impact normal industrial use of RFID.

In some locations, of course, it will be desirable and appropriate for RFID readers to scan private tags. Home appliances should contain RFID readers capable of scanning private tags. RFID readers that scan tags for item returns in shops might likewise have this capability, if consumers want it. (These readers, however, would need special restrictions on their use and, ideally, physical protections like metallic shielding and visible identifiers.)

With proper RFID reader configuration, the privacy bit strikes an attractive balance between privacy and utility. To ensure this balance, there is a need to enforce proper reader configuration and to defend against rogue readers used intentionally to infringe privacy.

A palette of technological tools can help. To support these tools, there needs to be a supplementary (and optional-to-deploy) RFID read command, which we might call private-read. A tag with its privacy bit turned off will respond to an ordinary read command; a tag with its privacy bit turned on will respond only to a private-read command.

The private-read command enables a few different approaches to privacy enforcement:

Audit. The simplest way to ensure the correct configuration of RFID readers is to check up on them. Thanks to the private-read command, this is a simple matter. In order to scan private tags, a reader must transmit a private-read command; it thereby publicly broadcasts its behavior. Special-purpose audit devices can detect the emission of a private-read command and identify readers that scan private tags. In fact, a properly configured RFID reading device can itself audit other readers; RFID readers might check up on one another. Once mobile phones come equipped with the right RFID functionality—a seemingly inevitable trend—they might alert their owners to the fact of private scanning taking place, facilitating a kind of citizen's watch network for RFID privacy.

Blocking. Reader auditing detects violations as they occur, or after the fact. A technological tool known as a **blocker tag** or blocker, on the other hand, can prevent privacy violations before they occur. A blocker effectively jams readers that emit private-read commands. In a nutshell, when it detects a private-read command, it simulates all possible RFID tags in the world, rendering the reader incapable of communicating with other tags. (To give a brief technical gloss for the EPC Gen 2 environment, a blocker tag would simulate collisions in all of the timeslots of the anticollision protocol.)

By carrying a blocker, a consumer can ensure against scanning of her personal possessions. When she wants private items to be scanned—in the home for example—she need merely remove her blocker tag from their vicinity. For example, if the consumer has a blocker tag mounted on the outside of her pocketbook, it will confer privacy protection while she is walking in the street. When she puts her RFID-tagged garments in a smart, RFID-enabled washing machine, though, the blocker will have no effect.

Blocker tags are just a research concept at present. They could, however, assume a form similar in size and cost to ordinary tags, and might even be embedded in shopping bags. Alternatively, to ensure easier management and more consistent signal strength, a blocker might be realized in a powered device like a mobile phone.

Blockers, of course, are selective in the sense that they have no impact on the scanning of tags whose privacy bit is off. This special, critical feature means that blockers would have no effect on ordinary industrial RFID readers.

Policy. Technology works most effectively in concert with well-crafted policy. Laws or guidelines around the appropriate use of private RFID scanning would benefit technological aids like the privacy bit.

Researchers with the Auto-ID Lab at the University of St. Gallen and ETH Zurich have enunciated ideas similar in spirit to the privacy bit, and have investigated both enforcement via audit devices and the relationship of their ideas to the Organization for Economic Cooperation and Development's guidelines for protecting personal information (see [Scanning with a Purpose—Supporting the Fair Information Principles in RFID Protocols](#)).

The privacy bit is a technical springboard for privacy enhancement. No doubt technologists and policy makers will be able to develop many other ways to exploit and build upon it.

Technical realization of the privacy bit

Realization of the privacy bit as a supplement to EPCglobal's Gen 2 standard would be technically straightforward. The privacy bit would of course reside in an EPC tag as an additional logical bit of memory. (As it would serve only to control the response of the tag to the read and private-read commands, the privacy bit would not need to be memory-mapped.)

The kill command in the EPCglobal standard then provides a ready vehicle for secure flipping of the privacy bit. The standard designates three bits within the kill command whose function is as yet unspecified. (They are "reserved for future use.") One of these three might serve as a privacy-control bit. It would function as follows. When a reader issues the kill command with the privacy-control bit off, the result is an ordinary kill operation that permanently disables the tag. When a reader issues the kill command with the privacy-control bit on, however, no killing takes place. Instead, the kill command merely flips the privacy bit. For the easiest and most inexpensive deployment, the privacy bit could be one-time writeable, that is, subject to a single flip from off to on. For situations that require reuse (e.g., for EPC-tagged library books), tags might support multiple changes to the privacy bit.

The EPCglobal standard requires that the kill command be activated by means of numerical code unique to each tag. The operation of flipping the privacy bit would naturally inherit this security feature. Such protection is important, as wanton flipping of privacy bits would be just as bad as wanton killing of tags.

As an option in the EPCglobal standard, the privacy bit would have one very attractive feature: It would impose no cost on tag vendors that choose not to implement it. A vendor could produce tags that do not contain a privacy bit and do not recognize the private-read command (or, alternatively, always recognize it). Such tags would function normally in commercial environments, and might be killed at the point of sale, if desired.

A stitch in time saves nine

There is a broad recognition in the RFID industry that tagging of retail articles is some years away. It is tempting to put off contemplation of the privacy bit and kindred ideas for consumer privacy protection in favor of more immediate RFID deployment problems. This would be shortsighted.

While item-level tagging may be a distant prospect, pivotal policy discussions on RFID privacy are

afoot. A recent flurry of state-level legislation has focused on RFID; early bills have died, but pending ones may not. Attention within the governments of the United States and the European Union is mounting. The RFID industry must demonstrate forethought if it is to avoid the heavy hand of legislative regulation.

While EPC tags may not percolate into retail settings in the near term, consumers are already carrying RFID tags that pose privacy and security problems. Automobile immobilizers, proximity cards, and Speedpass tokens, all RFID tags in the broad sense of the term, are already commonplace. They render the problems of privacy and security both palpable and immediate to consumers. E-passports and other RFID-enabled identity cards loom on the horizon. Some libraries have already started to tag books with RFID; it is only a matter of time before video stores and other rental operations do so. (Note that for loaned or rented items, tag killing is unworkable, as a tag must last the lifetime of the article it is attached to. The privacy bit or a like solution will be essential.)

Most vital is the problem of legacy infrastructure. The RFID systems that we design today will last for decades; we will have to live with the security choices we make now. The security problems that bedevil the Internet today are instructive. Ten or 20 years ago, viruses, spyware and phishing were concepts of largely academic interest. Security features that might have prevented these problems seemed unjustified in the short term, and the architects of the Internet omitted them. The resulting flaws are today threatening to cripple Internet commerce. (In 2004, phishing in the U.S. alone produced industry losses estimated at \$1.2 billion.) These security problems on the Internet are costly, but there is a cause for hope: The software by which users connect to the Internet can be updated or patched. Retooling billions of little wireless hardware devices would be a more strenuous exercise.

Mistakes in Internet security have provided excellent schooling for the RFID community. We are now well placed to avoid the mistakes of the wired world as we lay the foundations for a new wireless one. It is to be hoped that EPCglobal and other industry bodies will rise to the challenge, and that the privacy bit and kindred concepts will smooth the way.

Ari Juels is manager of applied research at [RSA Laboratories](#) and a coinventor of the privacy bit and blocker tag. Technical papers on these ideas are available at www.rsasecurity.com/go/rfid. To comment on this article, click on the link below.