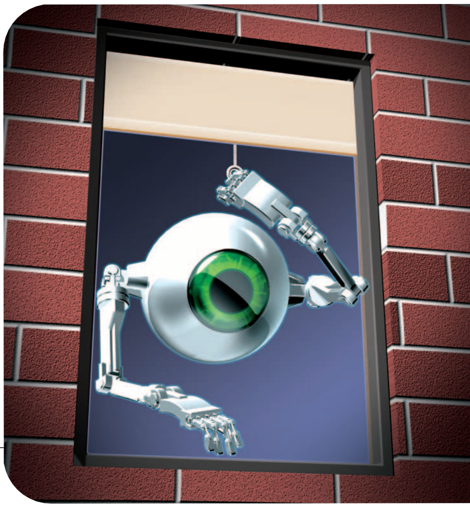
RFID Privacy: An Overview of Problems and Proposed Solutions

As organizations aggressively deploy Radio Frequency Identification systems, activists are increasingly concerned about RFID's potential to invade user privacy. This overview highlights potential threats and how they might be addressed using both technology and public policy.



SIMSON L. GARFINKEL
Massachusetts Institute of Technology

ARI JUELS
RSA Laboratories

RAVI PAPPU
ThingMagic

Tiny integrated circuits equipped with radio antennas are fast becoming one of the most controversial technologies ever to enter the consumer marketplace. These so-called Radio Frequency Identification tags—better known as RFID—could help stamp out drug counterfeiting, trace contaminated beef products to the very shelves where they reside, and eliminate supermarket checkout lines.

Yet, despite the technology's current widespread use and significant future potential, most popular press coverage of RFID tags has centered on the technology's potential for tracking consumers without their knowledge or consent. Typical of this coverage is a *Wired News* article that erroneously reported clothing giant Benetton's plans "to weave radio frequency ID chips into its garments to track its clothes worldwide."[1]

For RFID manufacturers, these tiny chips are the 21st Century replacement for the Universal Product Code bar codes developed in the 1970s. RFID tags offer an improved enumeration system, giving each tag at least a 96-bit number that is both globally unique and unreusable. But, unlike barcodes, RFID tags can be read at a distance without a person's knowledge. As a result, tags placed in consumer items for one purpose might be covertly used to track people as they move through the world. This is especially true of RFID tags that might be embedded in items such as shoes and clothing.

Some industry insiders discount such privacy concerns. Others say they can be trivially addressed using technologies that "kill" RFID chips when tagged items are sold to consumers. We believe that that privacy concerns are real and will only be solved by combining technical and policy approaches. We also believe that RFID can offer powerful benefits for businesses and consumers alike. If industry fails to address privacy concerns, however, these benefits might well be stymied by restrictive legislation or a public backlash.

RFID deployment

News reports on RFID privacy rarely point out that the technology has already been massively deployed throughout the US and much of the industrialized world. In November 2003, Mario Rivas, executive vice president for communications at Philips Semiconductors, said that Phillips had shipped more than a billion RFID devices worldwide. Mark Roberti, editor of *RFID Journal*, estimates that between 20 and 50 million Americans carry an RFID chip in their pocket every day—either in the form of a proximity card for entering buildings and garages or in an automobile key with an "immobilizer" chip molded into the key's plastic handle.

Current applications

RFID was first used during the Second World War in Identification Friend or Foe systems onboard military aircraft. Soon after, Harry Stockman demonstrated a system energized completely by reflected power.[2] The first Electronic Article Surveillance anti-theft systems were commercialized in the 1960s. In the 1970s, the US Department of Energy investigated the technology's potential to safeguard materials at nuclear weapons sites.

Today, RFID is used in a wide variety of applications, from remote keyless entry for automobiles to animal tracking, highway toll collection, and supply-chain management. This broad range of applications highlights an often-overlooked fact: the risks to personal privacy and data security vary greatly depending on the specific RFID system.

Automobile immobilizers. In these systems, the car key incorporates a passive RFID tag that the steering column authenticates, thereby enabling vehicle operation. The tags are usually factory programmed and cannot be rewritten in the field. Some versions include cryptographic communications between the key and the steering column.

Immobilizers have a small read range (typically 5 cm), operate in the low-frequency end of the electromagnetic spectrum (between 125 and 134.2 KHz), and cost a few dollars each. Widely credited with reducing auto theft by as much as 50 percent[3] these systems are probably the best-known examples of RFID deployment translating into a measurable end-user benefit.

Animal tracking. Organizations and individuals are increasingly equipping pets, livestock, exotic animals, and endangered species with RFID tags to enable tracking, recovery, and management. In the US, many domestic cat and dog owners have RFID chips implanted in their pets. In August 2000, the Los Angeles City Council adopted a measure requiring that all animals adopted from the city's animal shelters have a microchip implanted at a cost of US$15 per animal.[4] Because the shelters also have RFID readers, lost animals recovered by a shelter can be easily returned to their owners. RFID chips are also being increasingly embedded into ear tags affixed to cattle. As another example, researchers have tracked dolphins and other marine animals with systems combining a GPS receiver with a radio transmitter that can be picked up by satellite (which costs approximately $4,000 per tag).

Payment systems. RFID tags are being used as credit-card-like payment tokens that contain a serial number. A reader sends the number over a network and a remote computer debits value from the consumer's account. To make fraud more difficult, some systems combine the serial number with a simple challenge–response protocol. One of the most popular RFID payment systems is Texas Instrument's Speedpass pay-at-the-pump system, introduced in Mobil stations in the mid-1990s. Several years ago, the European Central Bank purportedly considered embedding RFID tags into currency.[5]

Automatic toll collection. Highway authorities in many metropolitan areas now let travelers pay tolls using RFID tags linked to debit accounts. One of the most popular is E-ZPass, first used widely in New York. E-ZPass is based on a 921.75 MHz semi-passive tag with a shelf life of about five to seven years and a read range of several meters. The tags can be read as cars move up to 100 miles per hour, making it possible to use the tags for traffic monitoring and other applications. Several million US consumers are now using these tags nationwide.

Inventory management. For many, inventory management is the "holy grail" of RFID deployments. Individually serialized RFID tags are already being affixed to some consumer goods' packaging at the factory, then used to track packages as they get on the truck, travel by boat, arrive in a foreign country, leave the boat, enter the supply chain, travel through distribution, and eventually reach their in-store destinations. Tags can assure that products produced and sold in one market are not illegally diverted to another. Further, "smart shelves" equipped with RFID readers could integrate with inventory systems, tracking all merchandise and alerting store personnel when items are misshelved. RFID tags might even be used after the sale, for example, to ensure that consumers actually bought items that they're attempting to return or have serviced.

RFID potential (and potential problems)

Several other developments promise a dramatic increase in RFID's near-term deployment:

- Many suppliers have recently begun embedding RFID tags in cases and pallets of consumer goods sent to Wal-Mart and the US Military to make goods scannable by automatic inventory-control systems.
- Within a few years, RFID tags will be embedded in automobile tires to allow precise tire tracking in the event of a recall. This tracking capability was mandated in the November 2000 Transportation Recall Enhancement Accountability and Documentation (TREAD) Act, passed in the wake of the Firestone/Ford scandal.
- Zebra Technologies, one of the world's leaders in label and barcode printing, has developed a "print engine" that can embed an RFID transponder directly into a product label.[6]
- Hitachi has developed 0.4mm-square RFID tag called the "μ-chip" designed to be embedded into photocopier paper to enable automatic document tracking.[7]

Some privacy activists see RFID's widespread and unrestricted deployment as a kind of doomsday scenario in which corporate and government interests can pervasively track individuals—paving the way for a techno-totalitarian state in which each person's movements, associates, and casual acquaintances are carefully monitored and recorded in futuristic data centers. One of the leading crusaders here is Katherine Albrecht, director of Consumers Against Supermarket Privacy Invasion and

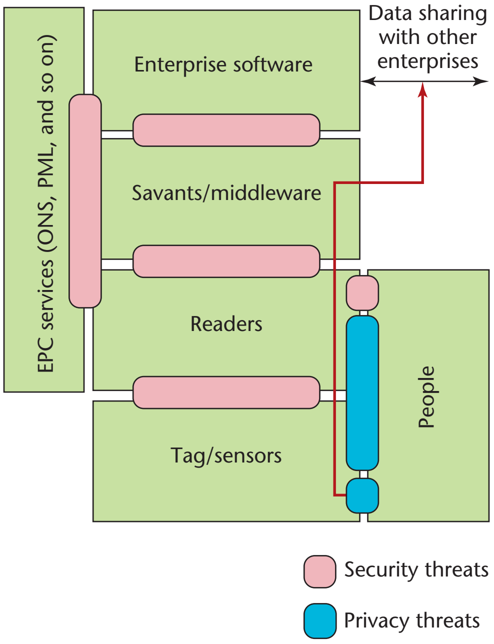


Figure 1. An abstract view of the EPC Network. The network defines standards for communication between tags and readers, and a set of EPC services, such as the Object Name Service (ONS) and Product Markup Language (PML), that enable scalable RFID networks. Pink boxes identify the location of threats to data security and blue boxes identify threats to personal privacy. The heavy red line calls out a special threat to personal privacy: the linking of personal identity to a set of unique tags. As personal identity moves up the stack and is stored and shared between enterprises, it becomes increasingly difficult to dissociate one's identity from the set of tags.

Numbering (Caspian). Albrecht variously calls RFID tags "spy chips" and "tracking devices"; she organized a Benetton boycott that forced the company to officially repudiate any RFID testing plans.

In November 2003, civil liberties organizations—including the Privacy Rights Clearing House, the American Civil Liberties Union, Caspian, and several academics (including an author of this article)—published a "Position Statement on the use of RFID on Consumer Products"[8] that was highly critical of RFID. According to the statement, if "used improperly, RFID has the potential to jeopardize consumer privacy, reduce or eliminate purchasing anonymity, and threaten civil liberties." The statement called for halt to RFID deployment until the technology could undergo a formal technology assessment.

Although RFID poses legitimate privacy concerns, the degree and nature of the technology's threat to privacy are easily misunderstood. To clarify these privacy issues, knowledge of RFID's technical characteristics and uses is essential.

RFID and the EPC network

Most RFID systems operate in the radio spectrum's unlicensed portion, where regulations govern power output for readers. This characteristic, combined with physical limitations, limits the reading range for *passive tags*, which are powered by the radio signal that reads them. Some passive tags operate in the low-frequency band (125–134.2 KHz), such as proximity cards and implantable glass-covered transponders. These devices have a typical read-range of less than two feet. Passive tags operating in the UHF band (915MHz in North America) can typically be read at 10 meters or more in free space, but the range diminishes when tags are attached to everyday objects. Also, human beings absorb UHF radiation and disrupt the communication between passive tags and readers. *Active tags* are battery-equipped and have longer ranges, but they are also significantly more expensive and have a limited shelf life.

Although different RFID systems have been in use for years, popular accounts of RFID technology typically refer to the Electronic Product Code. The EPC was developed by the Auto-ID Center in collaboration with the Massachusetts Institute of Technology and other universities, and is now managed by EPCglobal. The center's goal was to make RFID tags as simple as possible, with the aim of driving the chips' price below five cents. Working with industry partners such as Procter & Gamble, the Auto-ID Center developed an RFID system that many in the industry hope will replace the ubiquitous Universal Product Code bar codes present on many consumer products.

Each EPC tag has a serial number of at least 96 bits divided into sections identifying the tagged item's manufacturer, product, version, and serial number. In addition to being an identification code, this number can serve as a pointer to a database entry for the tag that contains a detailed transactional history for the associated object. For example, EPCglobal is in the process of elaborating a universally accessible Object Name Service (ONS) database; this service will provide information about tagged objects. Unlike today's proprietary and mutually incompatible RFID systems, EPC is being promoted as a single, open worldwide RFID standard that will dramatically lower costs and increase adoption. Figure 1 shows an abstract view of the EPC Network.

EPC tags contain several thousand transistors and a small antenna. Given the small size, the most inexpensive emerging generations of these tags will likely have only between 250 and 1,000 gates available for security features.[9] As a result, they won't implement encryption algorithms or other traditional security features. EPCglobal has recently completed its Class-1 Generation-2 EPC tag standard, which is likely to see widespread deployment in the coming years. In this standard, tags contain a *kill* self-destruct feature. When an EPC tag successfully receives

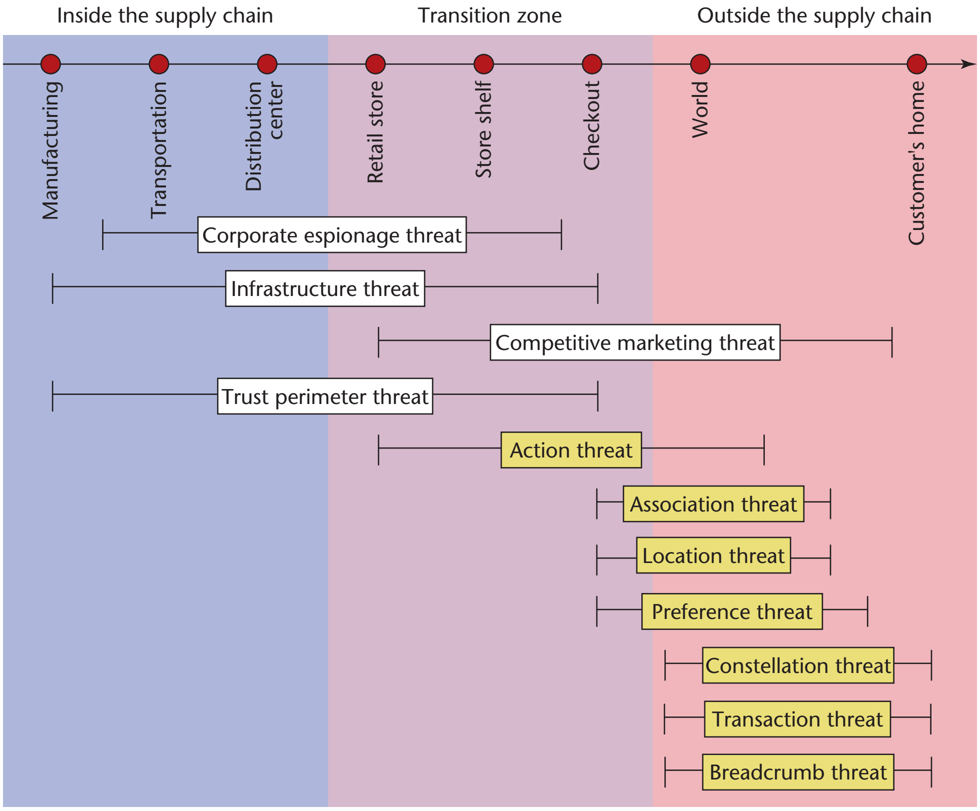


Figure 2. Threat contexts in EPC deployment. Labels in white indicate threats to corporate data security, whereas threats in yellow are threats to personal privacy.

the kill command, it renders itself permanently inoperable. To prevent inadvertent or malicious disablement of tags, the EPC-standard kill command requires readers to use a tag-specific, 32-bit password.

RFID privacy and security risks

RFID technology poses unique privacy and security concerns because humans cannot sense the RF radiation used to read tags, and the tags themselves typically maintain no history of past readings. As a result, tags are promiscuous: they can be read by entities other than their owners and without their owners' knowledge. Further, both tags and readers can be covertly embedded in the environment; short-range readers can be small enough to fit into a cell phone.[10]

Figure 2 identifies the major contexts for EPC tags:

- *Inside the supply chain*, including factories where tagged objects are manufactured, transportation systems, and retail store back rooms.
- *The transition zone*, including customer-facing portions of retail stores, where tagged items change hands from the vendor to the customer.
- *Outside the supply chain*, including all locations up to and including customer homes.

Threats can be further divided into those primarily affecting corporations and other organizations (white labels in Figure 2), and those primarily affecting individuals (yellow labels).

Corporate data security threats

EPC poses a threat to corporate data security because many different parties can read tags. We've identified four threats here:

- *Corporate espionage threat*. Tagged objects in the supply chain make it easier for competitors to remotely gather supply chain data, which is some of industry's most confidential information. For example, an agent could purchase a competitor's products from several locations, then monitor the locations' replenishment dynamics. In some scenarios, they could read tags in a store or even as the merchandise is unloaded. Because tagged objects are uniquely numbered, it's easier for competitors to unobtrusively gather large volumes of data.

- *Competitive marketing threat*. Tagged objects make it easier for competitors to gain unauthorized access to customer preferences and use the data in competitive marketing scenarios.
- *Infrastructure threat*. This is not a threat specific to RFID per se. However, a corporate infrastructure that's dependent on easily jammed radio frequency signals makes organizations susceptible to new kinds of denial-of-service attacks. Such attacks could be especially devastating as RFID becomes a mission-critical component of corporate infrastructure.
- *Trust perimeter threat*. Although not specific to RFID, as organizations increasingly share larger volumes of data electronically, the sharing mechanisms offer new opportunities for attack.

Personal privacy threats

Most personal privacy threats arise from the fact that tags with unique IDs can be easily associated with a person's identity:

- *Action threat*. In this threat, an individual's behavior (or possibly his or her intent) is inferred by monitoring the action of a group of tags. Some manufacturers of "smart shelves," for example, have suggested that the sudden disappearance of tags corresponding to several high-value objects might indicate that a person plans to shoplift, and could result in the person's photograph being taken. However, said tags might also disappear if the person accidentally knocked the tagged objects to the floor.
- *Association threat*. When a customer purchases an EPC-tagged item, the customer's identity can be associated with the item's electronic serial number. This threat is fundamentally different than the current practice of associating customer loyalty cards with purchases, because the EPC associates the consumer with a specific item (a unique aspirin package) rather than with a class of items (an aspirin package). Also, unlike with loyalty cards, this type of association can be clandestine and even involuntary.
- *Location threat*. Placing covert readers at specific locations creates two types of privacy threats. First, individuals carrying unique tags can be monitored and their location revealed if the monitoring agency knows the tags associated with those individuals. Second, a tagged object's location—regardless of who (or what) is carrying it—is susceptible to unauthorized disclosure.
- *Preference threat*. With the EPC network, the tag on an item uniquely identifies the manufacturer, the product type, and the item's unique identity. This exposes otherwise unavailable customer preferences to competitive (and inquisitive) forces at low marginal cost. This is also a *value threat* if the adversary can easily determine the item's monetary value. A common example of this threat is a thief who targets victims based on their preferences (such as for high-value RFID-containing watches rather than low-cost ones).
- *Constellation threat*. Regardless of whether individual identity is associated with a tag set or not, the tags form a unique RFID shadow or *constellation* around the person. Adversaries can use this constellation to track people, without necessarily knowing their identities.
- *Transaction threat*. When tagged objects move from one constellation to another, it is easy to infer a transaction between the individuals associated with those constellations.
- *Breadcrumb threat*. This threat is also a consequence of association. As individuals collect tagged items, they're building an items database associated with their identity in corporate information systems. When they discard these *electronic breadcrumbs*, the association between them and the items isn't broken. The threat arises when discarded breadcrumbs are used, for example, to commit a crime or some other malicious act. The only identity associated with the breadcrumb is that of the original owner, who is liable, at the very least, to be bothered by law enforcement.

The cloning threat

Researchers at Johns Hopkins University and RSA Laboratories recently identified a serious security weakness in the RFID tag in Speedpass devices and many automobile immobilizer systems.[11] By demonstrating that such tags could be cloned, the researchers revealed the possibility of payment fraud and new modes of automobile theft. Although their discovery doesn't directly undermine consumer privacy, it demonstrates that RFID tags could have security consequences beyond merely tracking or profiling consumers.

Technical solutions

It would be ideal if we could address RFID's privacy and security threats by making minor modifications to the technology itself. Technical solutions have great appeal. Implementation and testing costs are fixed and up-front. Once developed, the solutions can be directly integrated into the product and usually require little user education or regulatory enforcement.

Indeed, the Auto-ID Center explicitly designed the EPC kill command as a pro-privacy technology. The designers realized that EPC tags might be irretrievably embedded in consumer devices and that consumers might not want to be tracked. They viewed killing EPC tags at the point-of-sale as an easy way out of the apparent privacy dilemma. The underlying principle is that "dead tags don't talk." As an alternative to killing, tags can also be attached to a product's price tag and discarded at the point-of-sale.

Why killing isn't enough

Activated tags can have a post-sale value to consumers, so simply killing or removing them when products are purchased is not a cure-all for the RFID privacy problem. In addition to facilitating item returns or repairs, there are numerous other possible practical uses for RFID tags.

People who are physically or mentally impaired might benefit from RFID-based home aids that use tag information.[12] For example, a personal RFID reader could help blind people by reading labels to reveal product contents. There are also industry plans afoot to provide mobile-phone-based readers,[13] which could let consumers scan RFID-tagged movie posters to learn show times, for example. Consumers could use these same readers to scan their own RFID tags and catalog their possessions. Also, if companies routinely kill tags at the point-of-sale, RFID-enabled "smart" consumer appliances—such as refrigerators that can identify expired or depleted foodstuffs—wouldn't work, killing a promising market along with the tags.

Regardless of whether EPC tags are routinely killed at the point-of-sale in retail situations, live RFID tags are already proliferating in everyday life. Conspicuous examples include contactless (wireless) smartcards, automated-toll-payment plaques, proximity cards, and automobile immobilizer chips.

Tag killing also fails to address the privacy of commercial users. As currently envisioned, RFID tags pose a considerable threat of industrial espionage.[14] The threat exists even for the limited, pallet-level deployments planned by many industries and mandated by Wal-Mart and the US Department of Defense. Disabling or removing tags at the point-of-sale does not address this problem at all.

The encryption option

As an alternative, cryptography provides some measure of privacy. Storing encrypted serial numbers on tags initially seems like a viable approach to privacy protection. It introduces two problems, though. First, there's the problem of key management. How will the corresponding *decryption* key be distributed and managed? Second, simple encryption doesn't solve the tracking problem. An encrypted serial number is itself a kind of meta-serial number—namely, a static identifier that can be used to track an RFID tag's possessor.

Could the tag itself perform dynamic, onboard cryptographic operations? The main obstacle here is cost. Most nontrivial cryptographic algorithms would unacceptably inflate the price of low-cost RFID tags, particularly the type envisioned for supply chain use. In this case, Moore's law doesn't hold forth its usual promise of inexorable increases in computing power. While five-cent RFID tags will no doubt be capable of increasingly powerful computation, commercial pressures will push the industry to using one-cent tags when they become available, rather than keeping the tag price at five cents and adding advanced cryptographic features.

Some researchers have proposed performing cryptographic operations on readers and storing the resulting information in tags.[15,16] However, as the following approaches illustrate, there are several practical ideas that don't require using cryptography in reader-tag protocols.

Tag passwords

Basic EPC RFID tags have sufficient resources to verify PINs or passwords. At first glance, this appears to be a possible vehicle for privacy protection: A tag could emit important information only if it receives the right password. The paradox here is that a reader can't know which password to transmit to a tag unless it knows the tag's identity.

Passwords might still prove useful in certain environments. For example, retail stores could program tags at checkout to respond to a particular password *P* emitted by the RFID network in a consumer's home. This would protect consumers' privacy between a store and their homes. If consumers want to use RFID tags in multiple environments, however, they'd face a thorny password-management problem.

Tag pseudonyms

Rather than be programmed with passwords, RFID tags could maintain consumer privacy simply by changing their serial numbers. One basic implementation would be to give each tag a set of pseudonyms p_1, p_2, … p_k and have the tag cycle through them each time it's read.

Unauthorized tag tracking would be more difficult, because potential adversaries wouldn't know that two different pseudonyms, p_i and p_j, belong to the same tag. The tag's owner, on the other hand, would have a list of all the tag's pseudonyms, and the tag could be identified whenever it was queried. However, attackers could repeatedly scan the same tag, thereby forcing it to cycle through all available pseudonyms. As a countermeasure, tags could *throttle* the queries they receive. For example, a tag might release a new pseudonym only every five minutes. This would make it harder for a reader to harvest all of a tag's pseudonyms when the owner is walking down the street.

As currently envisioned, RFID tags pose a considerable threat of industrial espionage.

Making tag serial numbers reprogrammable offers other possibilities. An authenticated, trusted reader could randomize or otherwise refresh a tag's serial number. Given an adequately large code space of unique identifiers—such as 96-bit random serial numbers—it's highly unlikely that two tags would be programmed with the same randomly chosen number.

A sophisticated adversary might well be able to design or configure a reader that sometimes defeats blocker tags.

Pseudonym management is especially attractive in environments where one of the main threats is passive eavesdropping on readers. Suppose that each tag carries two random pseudonyms, p_1 and p_2. If Warehouse A scans p_1 only, and Distributor B scans p_2 only, eavesdroppers will not know when they're detecting the same RFID tag in both locations because they'll intercept only seemingly unrelated pseudonyms. Provided that the warehouse and the distributor share pseudonym information over a secure, back-end channel, the two-pseudonym scheme lets them transparently identify RFID tags on shipped items. (A lengthy discussion of RFID pseudonym management is available elsewhere.[15])

Blocker tags

The RFID blocker tag[17] takes a different approach to enhancing RFID privacy. It involves no modification to consumer tags. Rather, the blocker tag creates an RF environment that is hostile to RFID readers. The blocker tag is a specially configured, ancillary RFID tag that prevents unauthorized scanning of consumer items. In a nutshell, the blocker tag "spams" misbehaving readers so they can't locate the protected tags' identifiers. At the same time, it permits authorized scanners to proceed normally.

If two RFID tags simultaneously transmit their identifiers to a reader, a broadcast collision occurs that prevents the reader from deciphering either response. To avoid this problem, RFID readers and tags engage in *singulation*, an anti-collision protocol. An example is the *tree-walking* protocol, in which k-bit identifiers are viewed as binary tree leaves of depth k. In this tree, a node represents a binary identifier prefix. Its left child represents the prefix with a 0 appended; the right child, the prefix with a 1 appended. For a given tree node at depth I (representing an i-bit identifier prefix), the reader starts at the tree's root ($i = 0$) and asks all subtree tags to broadcast their next bit—that is, $(i + 1)^{st}$. If all tags broadcast a 0, then the reader recurses on the left subtree; if all tags broadcast a 1, then the reader recurses on the right. If some tags broadcast a 0 and some broadcast a 1, then the reader recurses on both subtrees.

The blocker tag spoofs the tree-walking protocol into thinking that all tags—that is, all identifiers—are present. To do this, it simply emits both a 0 and a 1 in response to all reader queries. The result is that the reader attempts to traverse the entire identifier tree, believing that all possible tag identifiers in the world are present! The reader stalls because the tree is far too big to be fully scanned (for Class 1 EPC tags, the tree would have 2^{96} nodes). It's likewise easy to construct a blocker tag that will disrupt an EPC reader. An EPC tag that doesn't totally disrupt all RFID activity requires a few refinements, however.

The first such refinement is to designate a *privacy zone*. This is a portion of the tree that the blocker simulates—say, the tree's right half, where all identifiers begin with a 1 bit. Tags to be protected by the blocker should then carry a leading 1 bit, whereas freely scannable tags carry a 0 bit. As a simple example, supermarket items might all carry tags with leading 0 bits, which would be flipped at the checkout register (when an appropriate PIN is provided). Supermarket bags could carry blocker tags, protecting the items from scanning until the consumer takes them home and removes them from the bags. At that point, if the items were placed in a "smart" refrigerator or similar device, their tags could again be scanned. With a *polite blocking* enhancement, the blocker tag would inform readers that it's present, so that they don't attempt to scan the privacy zone and subsequently stall.

A sophisticated adversary might well be able to design or configure a reader that sometimes defeats blocker tags. Blocker tags aim to enhance consumer privacy and make privacy violations more difficult, but they certainly provide nothing like foolproof protection. Also, impolite or even malicious blockers impose a denial-of-service threat. This threat is always present, however, and is not a good justification for refraining from polite blocker-tag deployment.

Soft blocking is an alternative, lightweight approach to blocker-tag deployment.[18] The basic idea is to enforce polite reader behavior by ensuring that they always adhere to a "blocker-compliant or "polite" policy. We might accomplish this by requiring that polite reader firmware be the commercial default, as well as using auditing procedures and legislative regulation. If readers adhere to a polite policy, a blocker tag can confer privacy protection merely by informing a reader of its presence. Thus, in the soft blocking approach, blocker tags might be ordinary RFID tags whose only special distinction is a special tag identifier, say, a *B* for blockers. This would make blocker tags especially easy to manufacture.

In soft blocking, a polite reader would begin a scan by checking for tags with the initial serial number *B*. If it detects *B*, the reader would refrain from scanning the privacy zone. This privacy zone respect would be directly auditable using a device that presents the reader with simulated tag sets and listens to the resulting reader signals. Soft blocking could support a flexible range of policies. For example, it could support an opt-in consumer privacy approach in which, by default, readers couldn't read private tags unless a special "deblocker" tag was present.

Soft blocking is similar to the P3P approach to Web privacy protection in that users issue explicit preference declarations, and it relies on a carefully regulated privacy enforcement environment. Soft blocking would not provide protection against rogue readers, just as P3P offers no strong technical barrier against information misuse. If desired, users could complement soft blocking with full-blown blocking.

Antenna-energy analysis

One approach to RFID privacy doesn't rely on logical protocols at all. Kenneth Fishkin and Sumit Roy have proposed a system based on the premise that legitimate readers are likely to be quite close to tags (such as at a checkout counter), whereas malicious readers are likely to be far away (such as a competitor in the parking lot).[19]

In preliminary experiments, Fishkin and Roy found that a reader signal's signal-to-noise ratio decreases measurably with distance. The farther away a reader is, the greater the noise level in the signal a tag receives. With some additional circuitry, therefore, an RFID tag might be able to obtain a rough estimate of the querying reader's distance and change its behavior accordingly. A tag interacting with a distant reader might only reveal the type of product it's attached to—a pair of trousers, for example. When interacting with a nearby reader, however, the tag might also reveal its unique identifier. A more sophisticated, multi-tiered approach is also possible, in which tags furnish increasing amounts of information as readers get closer.

Of course, distance alone doesn't provide an ideal trust metric. But distance could be combined with traditional access-control techniques—such as a challenge-response protocol between the reader and tag—to achieve a more comprehensive approach to RFID-tag privacy. Indeed, the distance-measurement approach is complementary to both blocker tags and pseudonyms.

Policy solutions

It may prove valuable also to address RFID privacy and security issues through policy and regulation. In general, policy-based solutions are hard to implement and change, but have the advantage of being based on behavior and intent. Indeed, there is a long history of regulating information technology use when privacy is infringed upon, beginning with the codes of Fair Information Practices that have emerged over the past twenty-five years, and including the 1970 Fair Credit and Reporting Act, the 1980 Organization of Economic Cooperation and Development's "Guidelines on the Protection of Privacy and Transborder Flows of Personal Information," and the 1995 European Union "Directive on the Protection of Individuals" regarding personal data process and movement.

Simson Garfinkel, one of the authors, has proposed an "RFID Bill of Rights"[20] that adapts the principles of fair information practices to RFID systems deployment. This bill of rights consists of five guiding principles for RFID system creation and deployment. Users of RFID systems and purchasers of products containing RFID tags have:

1. The right to know if a product contains an RFID tag.
2. The right to have embedded RFID tags removed, deactivated, or destroyed when a product is purchased.
3. The right to first-class RFID alternatives. Consumers should not lose other rights (such as the right to return a product or travel on a particular road) if they decide to opt-out of RFID or exercise an RFID tag's kill feature.
4. The right to know what information is stored inside their RFID tags. If this information is incorrect, there must be a means to correct or amend it.
5. The right to know when, where, and why an RFID tag is being read.

Together, items 1 and 5 mandate against covert RFID systems. To comply with item 1, organizations might include a prominently displayed logo on any RFID-tagged product. The fifth item is likely to be the most controversial in the list. To comply with it, organizations could post a sign wherever RFID readers operate. Likewise, they could declare a space to be free of RFID readers with similar placards. Other options include

- readers could emit a tone or flash a light when a reading occurs,
- the tag itself could emit a tone or flash a light, or
- a tag equipped with memory could count the number of times it has been read.

Most of these options would add to the tag's cost, either in the form of a battery or increased functionality. We could instead develop RFID reader detectors for concerned consumers. Such detectors could be cheaply made and equipped with real-time clocks and position-aware technology such as GPS. Although such detectors might not be a primary means for enforcing item 5, reader detectors—along with RFID jammers and blocker tags—might prove a powerful means for identifying organizations that fail to comply with these principles.

Item 2 addresses a consumer fear: that stores might offer no means to deactivate RFID tags. Tags that comply with the Auto-ID Center's standard will be required to incorporate a password-protected kill feature. Another approach would be to deploy tags that could erase their unique serial numbers at checkout, but retain other information.

Item 3's goal is to protect consumers who decline RFID-enabled services. It's easy to imagine how a poorly designed RFID system could be coercively deployed if consumers have no choice regarding its use. For example, if the only way to use a particular highway is by paying the toll with an RFID tag, then even consumers who are opposed to the tag might be forced to use it if alternative routes are unavailable.

Some RFID devices have limited read/write data storage; Item 4 is a straightforward application of fair information practices to any such system.

Declan McCullagh[21] has proposed more restrictive rules:

- Consumers should be notified when items they purchase contain RFID tags.
- RFID tags should be disabled by default at the checkout counter.
- RFID tags should be placed on product packaging instead of on the product when possible.
- RFID tags should be readily visible and easily removable.

Compliance with RFID regulations could be legislated or adopted voluntarily. If the latter, conformance with principles could be ensured through licensing logos, protocols, or intellectual property required for proper RFID operation.

RFID technology fits into the general landscape of geographically and identity-aware technologies that are currently being deployed. RFID, however, poses unique challenges because of its low cost and growing ubiquity.

As the awareness of RFID's utility has grown, so too has the chorus of consumer activists urging that the technology's deployment be delayed or abandoned. Increasingly, these activists have the ear of lawmakers. Unless RFID proponents can articulate a clear message that shows how RFID's promise can be realized without sacrificing privacy, it's possible that new regulations will significantly limit its usefulness.

The fact that the debate about RFID systems' privacy and security is taking place far ahead of the actual ubiquitous deployment is a good sign. We're hopeful that this debate will enable the evolution of both technology and policy in a reasoned manner, and will eventually allow the technology to be deployed without compromising personal privacy. □

Acknowledgments

The authors thank Mark Roberti, Dan Bailey, Steve Weis, and anonymous reviewers for their helpful comments on this article.

References

1. E. Batista, "What Your Clothes Say About You," *Wired News*, Mar. 12, 2003; www.wired.com/news/wireless/0,1382,58006,00.html/wn_ascii.
2. H. Stockman, "Communication by Means of Reflected Power," *Proc. Int'l Radio Eng. (IRE)*, IEEE Press, Oct. 1948, pp. 1196–1204.
3. Allianz Canada, "Allianz Canada Encourages Customers to Fight Auto Theft," 25 July 2001; www.allianzgroup.com/azgrp/dp/cda/0,,17111-44,00.html.
4. J. Kohlbrand, "Microchips Required for Adopted Animals," 7 Aug. 2000; www.worldnetdaily.com/news/article.asp?ARTICLE_ID=18758.
5. A. Juels and R. Pappu, "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes," *Financial Cryptography,* LNCS 2742, R. Wright, ed., Springer-Verlag, 2003, pp. 103–121.
6. J. Collins, "Zebra Unveils RFID Label Maker," *RFID J.*, 25 Sept. 2003; www.rfidjournal.com/article/articleview/592/1/1.
7. "Hitachi Unveils Smallest RFID Chip," *RFID J.*, 14 Mar. 2003; www.rfidjournal.com/article/articleview/337/1/1.
8. "RFID Position Statement of Consumer Privacy and Civil Liberties Organizations," 20 Nov. 2003; www.privacyrights.org/ar/RFIDposition.htm.
9. S.E. Sarma et al., "Radio-Frequency Identification: Security Risks and Challenges," *CryptoBytes,* Mar. 2003; www.rsasecurity.com/rsalabs/cryptobytes/CryptoBytes_March_2003_lowres.pdf.
10. "Nokia Unveils RFID Phone Reader," *RFID J.*, 17 Mar. 2003; www.rfidjournal.com/article/view/834.
11. S. Bono et al., "Security Analysis of a Cryptographically-Enabled RFID Device," to appear, *Usenix Security*, P. McDaniel, ed., Usenix Assoc., 2005.
12. M. Philipose et al., "Guide: Towards Understanding Daily Life via Auto-Identification and Statistical Analysis," *UbiHealth 2003: 2nd Int'l Workshop on Ubiquitous Computing for Pervasive Healthcare Applications*, Springer-Verlag, 2003; www.healthcare.pervasive.dk/ubicomp2003/papers/Final_Papers/16.pdf.
13. D. Thomas, "Nokia Brings RFID to Mobile Phones," 17 Mar. 2004; www.vnunet.com/News/1153568.
14. R. Stapleton-Gray, "Would Macy's Scan Gimbels?" RFID Privacy Workshop, MIT, 2003; http://whitepapers.zdnet.co.uk/0,39025945,60089924p-39000532q,00.htm.
15. A. Juels, "Minimalist Cryptography for RFID Tags," *4th Conf. Security in Comm. Networks* (SCN), C. Blundo and S. Cimato, eds., Springer-Verlag, 2004, pp. 149-164.

16. P. Golle et al., "Universal Re-encryption for Mixnets," *Proc. RSA Conference Cryptographer's Track* (CT-RSA), T. Okamoto, ed., Springer-Verlag, 2004, pp. 163–178.

17. A. Juels, R. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID tags for Consumer Privacy," *8th ACM Conf. Computer and Comm. Security*, V. Atluri, ed., ACM Press, 2003, pp. 103–111.

18. A. Juels and J. Brainard, "Soft Blocking: Flexible Blocker Tags on the Cheap," *Workshop on Privacy in the Electronic Society* (WPES 04), ACM Press, 2004, pp. 1–7.

19. K.P. Fishkin and S. Roy, "Enhancing RFID Privacy via Antenna Energy Analysis," tech. memo IRS-TR-03-012, Intel Research Seattle, 2003.

20. S. Garfinkel, "An RFID Bill of Rights," *Tech. Review*, October 2002; www.technologyreview.com/articles/02/10/garfinkel1002.asp.

21. D. McCullagh, "Are Spy Chips Set to Go Commercial?" 13 Jan. 2003; http://zdnet.com.com/2100-1107-980345.html.

***Simson L. Garfinkel** is a researcher in the field of computer security and a commentator on information technology. His research interests include computer security, the usability of secure systems, and information policy. Garfinkel received his PhD in electrical engineering and computer science at the Massachusetts Institute of Technology. Prior to joining CSAIL, Garfinkel founded Sandstorm Enterprises, a computer security tools vendor. He is coeditor (with Elisabeth Rosenberg) of* RFID: Application, Security, and Privacy *(Addison Wesley, July 2005). Contact him at simsong@acm.org.*

***Ari Juels** is principal research scientist at RSA Laboratories, where he oversees the various data security projects of the applied research program. While RFID security and privacy have been a recent emphasis of his research, he has also published papers on denial-of-service countermeasures, Internet privacy protection, electronic voting, biometric security, and user authentication. Juels has participated on the program committees of a number of technical conferences, and is currently program chair for the ACM CCS Conference Industry Track, program co-chair for PerComSec '06, and vice chair for the Security, Privacy, and Ethics track at WWW2006. Juels received his PhD in computer science at the University of California, Berkeley. In 2004, he was honored as one of* Technology Review*'s top 100 innovators under the age of 35. Contact him via www.ari-juels.com.*

***Ravi Pappu** is a cofounder of ThingMagic, a leader in the design of sophisticated RFID readers. His technical interests are physical cryptography, optical engineering, and display technology. He is also interested in low-cost computing for developing countries. Pappu holds a BS in electronics and communication engineering from Osmania University, India; an MS in electrical engineering from Villanova, and an MS in media arts and sciences and his PhD for inventing Physical One-Way Functions from the Massachusetts Institute of Technology. In 2003, he was honored as one of* Technology Review*'s top 100 innovators under the age of 35. Contact him at ravi@thingmagic.com.*