Adopting Fair Information Practices to Low Cost RFID Systems

Simson L. Garfinkel[1]

Laboratory for Computer Science

Massachusetts Institute of Technology
Cambridge, MA 02139

http://www.simson.net/

Presented at Ubiquitous Computing 2002 Privacy Workshop

Abstract. Within the coming years, low cost radio frequency identification (RFID) systems are expected to become commonplace throughout the business-to-business and business-to-consumer marketplace. Much of the work to date on these systems pertains to systems engineering and electronic product code issues. This paper discusses ways to ensure personal privacy, and presents policies and technologies that could limit abuse.

Introduction to RFID

"Automatic Identification" (Auto-ID) describes a wide class of technologies used for automatically identifying objects, individuals, and locations. Typical Auto-ID systems assign a code to a product model or type. This code can then be automatically read and manipulated by an information processing system. The Universal Product Code (UPC)/ European Article Number (EAN) bar code present on most consumer items sold in the world is one of the most widely used Auto-ID systems. Today more than 5 billion UPC/EAN codes are scanned world-wide on a daily basis [EAN02].

Auto-ID systems are expected to undergo two fundamental changes within the coming years. The first change will be the way that these codes are read and automatically processed; the second change involves the codes themselves. These issue must be addressed in the design, implementation and deployment of the system to protect the privacy of individuals.

From Optical Scanning to RFID. Instead of printed-on optical patterns that are read with an optical scanner, the next generation of Auto-ID systems will be based on electronic tags that are "read" using a wireless transceiver. These systems, collectively known as Radio Frequency Identification (RFID), have been increasingly used throughout the world in recent years.

RFID systems typically operate in the ISM and other free bands (9kHz-135 kHz; 13.56MHz; 868-870Mhz in Europe; 902-928Mhz in the US.) Tags can be *active*, which means that they are equipped with a power source for sending their responses, or *passive*, in which case they are powered by the reader. Active tags are more expensive, generally more reliable, and can have can be read over distances of several tens of meters. Passive tags are cheaper, less reliable, and can be read over distances ranging from a few centimeters to a few meters.[2]

RFID tags offer many advantages over traditional optically-scanned tags:

[1] simsong@mit.edu

[2] The Power consumption of the passive tag's electronics determines the range at which the tag can be read. For this reason, the industry has also developed *semi-active* tags that use an embedded battery to power the electronics, but which still employ passive response such as RF backscatter for uplink from the tag to the reader.

1. Optical barcodes need to be in plain view to be read; RFID tags can be read through fabric, paper, cardboard, and other materials that are transparent to the frequency of operation.
2. Traditional optical barcodes are limited to 13 digits of information, and two-dimensional barcodes are limited to several hundred; RFID tags can store hundreds or thousands of bytes of information.
3. Only a single optical barcode can be read at a time; dozens of RFID tags can be read at the same time with a single reader. For example, an RFID reader could be used to read all of the individually-tagged items within a case of merchandise.
4. Optical bar codes are read-only; advanced RFID tags can store information and perform limited processing.
5. Optical bar codes are *promiscuous*, in that any reader can read any compatible optical bar code that comes in range; RFID tags can be assigned a password, limiting who has the ability to read them.
6. The only way to deactivate an optical bar code is by obliterating or obscuring it; RFID tags can be electronically deactivated.

From Product Codes to Serial Numbers. Each UPC/EAN code is assigned by a manufacturer to a particular class of product. For example, the UPC "041508 800822" refers to a case of a dozen 750ml bottles of San Pellegrino sparkling natural mineral water. Each bottle inside the case has a UPC with the code "041508 800129." A shipping container might contain a thousand cases, all with the same code.

Each RFID tag, by contrast, can have its own unique identifying code. A shipping container of RFID-tagged San Pellegrino cases would have thousands of separate unique codes. One way of assigning these could be to use a standard UPC/EAN code as a prefix and to append a unique serial number. Such a system would allow easy integration with existing inventory systems, while simultaneously allowing new applications that make use of the unique ID.

RFID Today. RFID systems are now used for a variety of industrial and consumer applications, including access control, asset management, and warehouse automation.

Electronic toll collection and road pricing are a typical use of active and semi-active tags.[3] Automobiles are equipped with an active tag that can be read as the car moves through a toll booth or drives along the road. Each tag has a unique serial number; a database correlates the serial number with an account number that is automatically debited each time the tag is read [EZP02].

Implantable passive tags have seen significant use for tagging household pets. Stray animals that brought to shelters are scanned for a tag. If a tag is found, the name of the owner can be found by looking up the tag's serial number in a database [AVI02] [HAM02].

RFID Tomorrow. It is widely believed that RFID tags will migrate into consumer items as the price of tags drops to US$0.05 and below. For example, individually serialized RFID tags could be embedded into packages of high-value razor blades when the blades are manufactured. These tags could then be used to track the packages of blades are they are shipped from the factory through distribution and ultimately to retail shelves.

By giving each package a unique serial number, RFID would allow the manufacturer to:

? Keep track of material and assets in the supply chain, thereby reducing inventory.

? Pinpoint the location of theft (by determining that 1000 packages in 30 cases of razors that were scanned leaving a shipping dock were not subsequentially scanned when the cases were loaded onto a truck).

? Stop product diversion (when a shipping container of individually serialized batteries that were manufactured and labeled for sale in Hong Kong is scanned at the Port Authority in New York City).

[3] Passive tags can also be used for Electronic Toll Collection and road pricing.

? Stop importation of counterfeit consumer goods (even if the counterfeit goods contain an RFID tag, the serial number in the tag will not be registered as a genuine article.)

? Have more control over product recalls. Grocers could use an RFID scanner to rapidly locate tainted goods on store shelves; suspect serial numbers could be programmed into cash registers, to prohibit consumers from purchasing items that are blacklisted.

For consumers, some examples of the benefits of Auto-ID technology include:

? Compliance monitoring of medication dosage in elderly patients. (An RFID reader could note if a medicine bottle is taken out of the cabinet.)

? Alerting the consumer to product recalls. (Especially if there is a networked RFID reader at the door to the consumer's house.)

? Automatic replenishment of refrigerators and pantries.

? Ovens that can adjust themselves to properly cook prepackaged foods by reading their tags.

Amusingly enough, the application of finding lost keys in a cluttered house or apartment --- an application that has frequently appeared in popular accounts of RFID technology --- will probably *not* be a near-term application. Finding lost keys would require not only equipping a keychain with an RFID tag, but also equipping each room in a house with multiple RFID readers to allow for triangulation. Even then, the system might not be able to find keys that had fallen behind or into a couch or similar RF shields, unless the keys were equipped with active or semi-active tags.

Privacy Issues

Ubiquitous deployment of RFID tags in consumer products could pose several challenges to consumer privacy:

1. Tags could be read by unauthorized readers. (Although 13.56 MHz tags cannot be read from more than a meter away, unshielded passive 915 MHz tags can be read from many meters.)
2. Since human beings are not sensitive to radio signals, RFID tags could be read covertly.
3. A database could be used to build long-term tracking associations between tags and holders. Alternatively, such a database could simply be created at the checkout counter by correlating RFID tags with payment information. (Today this can be done with item info to track purchases made by an individual, but it is not currently possible to identify *which* consumer purchased *which* box of milk.)
4. The communication between the reader and the tag could be covertly monitored.

We can imagine several scenarios in which these properties could be exploited:

? A practical joker could covertly inventory, say, the undergarments of nearby pedestrians.

? Household electronics and other kinds of products might covertly inventory which other products are in the consumer's house, and then report this information back to a central repository—assuming that these "moles" have network access. Such information might be used to target the consumer for special offers, or to deny the consumer offers that he or she might otherwise receive.

? Additional unique identifiers could be stored into programmable RFID tags.

? A store could use a covert RFID reader to inventory the contents of a shopper's bags as they enter --- or even as they window shop. (In practice, such an application with a passive tag would be difficult, since paper can be an effective shield to some frequencies used by passive RFID systems.)

[SAR02] presents several technical measures for protecting the privacy of users, including:

1. At time of purchase, the tag could be either completely deactivated, or else the unique serial number could erased, leaving only the prefix.

2. Passwords could be assigned to the tags by the purchaser; this would prevent tags from being read without the owner's permission.

These measures depend on the consumer being aware of the existence of the tag and having the technical ability and the necessary patience to deactivate or reprogram an RFID tag. A lingering concern is that consumers might not be exercise these technical measures for any of a number of reasons:

? The manufacturer or merchandiser might wish to make future use of the tag.
? The consumer might not be informed of the tag's existence.
? Sufficient hurdles might be placed before consumers wishing to have a tag deactivated that, practically speaking, no consumers will exercise this option. (For example, consumers might be forced to purchase special equipment, or be required to call a phone number that is frequently busy to obtain an unlock code.)
? The manufacturer might not wish to go to the expense of purchasing tags that are reprogrammable or that have a "self-destruct" feature.

I believe that these problems can be solved through the use of policy and licensing requirements.

Fair Information Practices and the RFID Bill of Rights

Much current thinking on informational privacy issues is based on the Code of Fair Information Practices ([HEW73]), developed by the US Dept. of Health, Education in 1973.[4] The code has been subsequentially expanded in [OEC80] [EU95] and [CAN99].

We propose an "RFID Bill of Rights" which brings Fair Information Practices to deployment of RFID systems. The Bill of Rights consists of five guiding principles for the creation and deployment of RFID systems:

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: consumes should not lose other rights (e.g. the right to return a product or to travel on a particular road) if they decide to opt-out of RIFD 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 that there should be no covert RFID systems. One approach is to have a logo that must be prominently displayed on any product that contains an RFID tag and in any area that is under surveillance by RFID readers. Likewise, organizations that wish to declare a space "free" of RFID readers could have similar placards; freedom could be assured through the use of RFID reader detectors or RFID jammers.

[4] The Code of Fair Information Practices is based on five principles:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data. [HEW 73]

Item #2 overcomes the fear that stores might find it inconvenient to provide consumers with a means for deactivating their tags. Tags that comply with the Auto-ID Center's standard will be required to incorporate a password-protected "kill" feature. Rather than forcing consumers to find their passwords, are more consumer-friendly approach would be for manufacturers to use standardized kill passwords, or else to either kill tags or erase unique serial numbers as part of the checkout process.[5]

Item #3 seeks to avoid penalizing consumers who decline to partake in RFID-enabled services. It is easy to imagine how poorly-designed RFID system could be coercively deployed if consumers are not given a choice regarding its use. For example, if the only way to ride on a particular highway is by paying the toll with an RFID tag, than even consumers that are opposed to the tag might nevertheless use it, if there is no other way for them to commute to work.

Item #4 is a straightforward application of fair information practices to RIFD systems similar to the application of these principles to smartcards in [GAR99].

Item #5 is likely to be the most controversial. There are many ways that consumers can be informed that their RFID tags are being read. For example, a prominent placard could be placed in the vicinity of a reader. Readers could emit a tone or flash a light when a reading takes place. Alternatively, the tag itself could emit a tone or flash a light In addition, a tag equipped with memory could count the *number of times* that it has been read. Of course, a passive tag would not have an accurate time source to remember *when* the reading took place, and a simple count may not by itself add enough information. In general, though, most of these options would add cost to the tag, either in the form of a battery, or in the form of increased functionality.

Yet another alternative is providing concerned consumers with RFID reader detectors. 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, they could prove to be a powerful means for finding organizations that do not comply with these principles.

These principles could be legislated or could be adopted on a voluntary basis. If voluntary, conformance with the principles could be ensured through licensing of logos, protocols, or intellectual property required for proper RFID operation.

Conclusion

RFID is a powerful technology, and it is a technology that is likely to see world-wide deployment within the coming years. Attention to Fair Information Practices and related public-policy issues today will assure that these systems are designed and deployed in a manner that is compatible with evolving privacy principles.

Acknowledgements

Sanjay Sarma read several versions of this paper and contributed to the development of its arguments. I am indebted to him for his support.

[5] One potential problem with a widely-known "kill" password is the notion that a saboteur might enter a store for the purpose of killing all of the store's RFID tags. To protect against such actions, stores could be equipped with RFID sensing systems that will quickly report any such activity. Killing an RFID tag requires exercising anti-collision algorithms to find a particular tag, addressing the tag, and finally sending the "kill" command with sufficient power to affect a kill. Because of this involved procedure, even a high-speed RFID tag killing system would not be able to kill more than five tags per second. Such a system would have a distinct radio signature and would be easily found by a store with RFID readers in every aisle.

References

[AVI02] Avid Microchip Identification systems for animals, http://www.avidmicrochip.com/.

[CAN99] The House of Commons of Canada, 2nd Session, 36th Parliament, 48 Elizabeth II, 1999, Bill C-6, "Personal Information Protection and Electronic Documents Act."

[EAN02] "Note to Editors," EAN International and the Uniform Code Council, http://www.ean-int.org/index800.html

[EU95] European Union Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://europa.eu.int/comm/internal_market/en/dataprot/law/

[EZP02] E-ZPass Regional Consortium Service Center, http://www.ezpass.com/.

[GAR99] Garfinkel, Simson. "Smartcard holder's bill of rights." http://www.simson.net/smartrights.html.

[HEW73] U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens (1973).

[HAM02] Home Again Microchip Identification System, http://www.homeagainid.com/.

[MAL02] Mallory Sonalert Products, "Introduction to Sonalert Audible Signal Devices," http://www.mallory-sonalert.com/sonalert_audible_intro.htm

[OEC80] Organization for Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.

[SAR02] "Low Cost RFID and the Electronic Product Code," Sarma, S. E., Weis, S. A., Engels, D. W, Auto-ID Center, Massachusetts Institute of Technology, Cambridge, MA 02139. 2002