Enabling RFID in Retail

George Roussos
Birkbeck College,
University of London

Although currently impractical except for high-value products, item-level RFID tagging offers tangible benefits to both suppliers and retailers. However, widespread deployment will ultimately depend on public concerns about privacy protection.

The past two years have witnessed an explosion of interest in radio-frequency identification and supporting technologies, due primarily to their rapidly expanding use in tracking grocery products through the supply chain. Currently such applications monitor store-keeping units (SKUs) rather than individual goods, as the relatively high cost of RFID deployment and the very low profit margin of supermarket products make item-level tagging impractical.

Yet, economic and technical concerns aside, it is easy to envision a supermarket in which each item is tagged with an RFID label and all shopping carts feature RFID readers. The carts could potentially include onboard computers that recognize products placed inside and that display information and promotions retrieved wirelessly from the system back end. RFID-enabled smart phones, which are commercially available today and becoming increasingly popular, could carry out the same function.

Item-level deployment of RFID technology would also allow for quick checkout aisles that scan all products at once and thus eliminate queues, which are consistently reported as one of the most negative aspects of supermarket shopping. A simple extension of this system would be to embed RFID devices in consumers' loyalty or frequent-shopper cards to identify individuals. This could expedite system login and charge the shopping cost directly to the customer's account at the point of sale—unless removed at the POS, item-level tags will inevitably follow the consumer home. This scenario undoubtedly raises numerous privacy concerns.

RADIO-FREQUENCY IDENTIFICATION

RFID refers to any system that can transmit identification numbers over radio. Such systems have been around since the end of World War II, when the allies used an early version of the technology to distinguish friendly and enemy aircraft from a distance. Since then, RFID has been used in numerous applications including animal tracking, automatic toll collection, car immobilizers, and building access control systems.[1,2]

In recent years, however, public interest in such systems has grown rapidly due to various high-profile deployments that directly affect individuals in their daily activities.[3] RFID has evolved from an arcane business technology into a personal technology that affects everyone.

Supermarkets and other retailers across the world are planning large-scale item-level deployments in consumer goods that will leave few citizens in developed societies unaffected. Such implementations have found champions on every continent: Wal-Mart in the US, Marks & Spencer and Tesco in the UK, Metro in

Published by the IEEE Computer Society

Germany, Coles Myer in Australia, and Mitsukoshi in Japan are all leading retailers that are currently implementing RFID solutions across their supply chain. Moreover, under a US-led worldwide initiative, governments are using RFID to embed biometric information such as iris scans into passports to improve security.

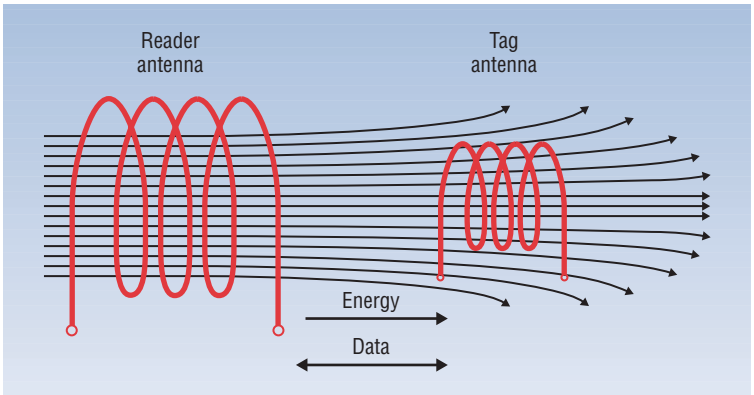

Figure 1. RFID operation. The reader antenna provides the power for the tag to transmit its stored identification number.

Operating principles

RFID systems have two parts: the tag and the reader. An RFID tag consists of a microcontroller, an antenna (either wire or printed using conductive carbon ink), and polymer-encapsulating material that wraps around the antenna and processor.

As Figure 1 shows, the reader initiates the identification process by generating an RF field at a specific frequency defined for the particular system, thereby causing a voltage difference at the tag antenna end points via inductive or capacitive coupling. The tag detects this change and, after optionally authenticating the reader via a challenge-response mechanism, responds by transmitting the identifier that it holds.

RFID tags can be passive or active depending on whether they are completely powered by the RF signal transmitted by the reader or they also carry an additional embedded power source. Each type has particular advantages.

Because they do not require a power source, *passive* RFID tags continue to operate until damaged or discarded. However, in normal operating circumstances they can be read only when the reader is within a few centimeters, and the data transmitted has a high error rate.

Active RFID tags, on the other hand, have a much longer range that can exceed 100 meters. Active tags provide more reliable communication, but they expire after their battery runs out—a period as long as seven years in some systems. Because they incorporate a battery, active RFID tags are significantly larger than passive tags.

In either case, a tag's actual transmission range depends on antenna size: A larger antenna provides a longer reading range.

Performance implications

An RFID system's operating frequency has considerable performance implications. For example, RFID-based security cards often operate between 125 and 134 Khz, where reading ranges are short but the RF signal is not significantly absorbed by water—a critical issue in this case, as the human body is mostly composed of water.

Modern RFID systems designed for supermarket use operate in the 800 Mhz (Europe) or 900 Mhz (US) range, offering longer reach and the much higher data rates required for certain operations—for example, to speedily record all items in a shopping cart for quick checkout aisles. However, at these operating frequencies, radio waves are easily absorbed by water or the thinnest layer of metal. Consequently, placing even a few soda cans in a shopping cart can prevent the accurate recording of products, making quick checkout unworkable.[4]

Privacy implications

Perhaps the most important implication of RFID technology today relates to its use within bigger information systems connected to the Internet: The identifiers retrieved from a tag can be used to query or update online databases that hold information about objects and people alike.

For example, given an electronic product code (EPC) retrieved from a supermarket item, the Object Naming Service directory will locate and obtain information about this product that the manufacturer publishes via the EPC Information Service, in much the same way that the Domain Name System provides data about individual Internet hosts. This information will relate to the particular item rather than the product class to which it belongs, as is the case with common bar codes.

Often, after a technology is deployed, new uses are discovered that may affect consumer privacy. For example, electronic toll collection systems have used active tags to record individual vehicles' speeds, ostensibly to help manage traffic, raising privacy concerns about drivers' locations.

The ability to silently retrieve and record product or personal identifiers, combined with the advanced, real-time information processing capability available today, have increased public uneasiness about the widespread use of RFID technology.

ITEM-LEVEL TAGGING IN RETAIL

Although the cost of both tag and reader is today too high to make item-level RFID tagging practical except for high-value products, it is a natural extension of supply-chain management principles, offering tangible ben-

efits to both suppliers and retailers. During the past three decades, successful implementation of several Efficient Consumer Response initiatives, which advocate the use of information technology to maximize consumer value and minimize supply-chain inefficiencies, have also boosted interest in RFID.

Vendor-managed inventory

One of the major ECR successes has been the *vendor-managed inventory* approach in which the vendor, rather than the customer, specifies delivery quantities sent through the distribution channel. VMI has become feasible because of two technologies: EDI supports automated electronic data interchange between trading partners, and bar codes offer standardized product identifiers.

Any retail RFID system necessarily involves tradeoffs between advanced functionality and privacy protection.

Using RFID at the SKU level further improves VMI efficiency by automating the manual scanning of stock, which enables continuous and accurate data flows for use by enterprise resource-planning (ERP) software and for optimized logistics. An extension of VMI first proposed in the mid-1990s[5] is to expand the supply chain to include the consumer home—arguably, the replenishment process begins when a product is consumed and its packaging discarded.

User profiling

Among other uses for item-level information, user profiling for effective price discrimination is most valuable to manufacturers and retailers. Every year, various industries invest considerable resources to attract and retain specific consumer groups with the long-term aim of providing individualized marketing and services—often referred to as *mass customization*.

Although direct individual marketing is not yet feasible, there has been rapid progress toward this objective in the last decade. One major UK supermarket chain has extended its clustering of customers from eight to 150 target groups using information collected via its loyalty club scheme, and provides different campaigns to address each group's needs.

RFID use is expected to provide new insights into consumer shopping habits and consumption patterns, and the organizations that can best exploit this information can expect to enjoy a significant competitive advantage. One measure of this new information's importance is that in 2005, all major ERP providers announced support of item-level recording in their products.

In particular, RFID use in a retail store creates an information trail that combines location recordings, routes through the store, and interactions with products. Retailers can aggregate and mine this data for patterns and consumer routines to help customers navigate the store—particularly important for mega-stores—and to develop individualized offers and promotions. For example, correlating cart content to individual demographics and lifestyle choices can form the basis for recommendations of specific products, such as food appropriate to a low-cholesterol diet, at a suitable price level. In addition, after-sales product traceability can assist in drug anticounterfeiting, medication compliance, and food monitoring and recall.

Other applications

Item-level RFID infrastructures also can be used to develop various useful applications not directly related to supply-chain management. For example, current best practice is to estimate stock levels, and thus replenishment strategies, using POS data; however, this frequently results in an 8 to 12 percent error, especially for retailers of fast-moving consumer goods. In the UK, Marks & Spencer has implemented item-level tagging of men's suits to achieve more accurate estimates, resulting in improved product availability and thus increased sales.

Other RFID applications emphasize the user experience. For example, Tokyo's Takashimaya department stores use item-level tagging to check the availability of specific sizes and colors of women's shoes. In addition, consumers use RFID-based cashless smart cards to pay for public transportation in several major cities including London, Paris, Hong Kong, and Tokyo.

CONSUMER PRIVACY PERCEPTIONS

My colleagues and I recently carried out extensive qualitative and quantitative research with a prototype item-level RFID retail system.[6] Study participants unanimously objected to any type of RFID recording or to the delivery of personalized commercial communications at home. They viewed both activities as direct privacy violations and valued control over system operation more than potential commercial opportunities.

The subjects understood that any retail RFID system necessarily involves tradeoffs between advanced functionality and privacy protection. However, this does not imply consumers would accept uncontrolled use of personal data—an aspect of the system that attracted significant criticism from the study participants, who observed that once it collected such data, a business could use it proactively in ways not directly related to the service provisions.

In fact, the vast majority of participants expressed an unwillingness to provide personal data unless they were confident it would be used fairly in the context of a particular service. Although they recognized that such a system would benefit businesses by reducing costs and more

accurately predicting the success of particular offers and promotions, they did not perceive the service as equally or even comparably valuable to consumers.

Using personal data beyond the expressed purpose of collection appears to violate the trust relationship between buyer and seller as well as the consumer's silent or explicit expectation that both parties do whatever possible to protect that relationship from outsiders. In fact, most consumers do not trust retailers to comply with the European Union's Data Protection and related privacy directives, discussed in more detail in the "Retail RFID and the European Regulatory Environment" sidebar, and they expect law to be their main guarantee against exploitation.[7]

Study participants were also uncomfortable with the notion of personal files that businesses could use to infer facts, habits, and routines about individuals. In the subjects' view, predicting user likes and dislikes is more intrusive than helpful. Such systems disrupt social practices and etiquette—for example, established familial roles and perceptions of polite behavior—and reduce shopping to a primarily mechanistic activity. In philosophical terms, they violate individuals' freedom of choice and sense of uniqueness.

PRIVACY PROTECTION TECHNOLOGIES

A recent attempt to address privacy concerns is the extension of the EPC protocol with the *destroy* command, which dictates when tags should permanently stop accepting further read requests. Although this feature is a step in the right direction, consumers still have no practical way to verify that tags have been disabled. Indeed, in recent trials at Metro supermarkets in Germany, POS disablers malfunctioned and users ended up with readable tags despite receiving notification that the operation had been carried out successfully.

Moreover, the destroy command is typically implemented in software and cannot withstand a hardware or

Retail RFID and the European Regulatory Environment

The European Union was established in 1992 as a loose partnership of countries aiming to promote safety and prosperity in the region through economic cooperation. In recent years, the EU has established a number of common policies guided by the Charter of Fundamental Rights (2000/C364/01), which outlines the civil, political, economic, and social rights of all European citizens and residents. In particular, Article 7 refers to the right of "respect for private and family life: right to privacy, home and correspondence."

Although the charter is a set of guiding principles with restricted legal powers (member states may or may not implement them as national law), several directives directly impact RFID in retail including the 1995 Data Protection Directive (95/46/EC), the 2000 Electronic Commerce Directive (2000/31/EC), and the 2002 Privacy and Electronic Communications Directive (2002/58/EC).

Data Protection Directive

This directive applies to the fair use of personal data—that is, "any information relating to an identified or identifiable natural person"—and affects "all the means likely reasonably to be used either by the controller [of the data] or by any other person."

The directive requires that data

- be collected only for specified lawful purposes and not beyond the intended scope of collection;
- be adequate, relevant, and not excessive in relation to the purpose of collection;
- be kept accurate and not longer than necessary; and
- not be transferred outside the European Economic Area unless a similar level of protection is ensured.

In addition, appropriate technical and organizational measures must be taken against unauthorized or unlawful processing. Further requirements restrict the use of sensitive personal data including that related to religion or sexual preferences.

Different member states have interpreted the Data Protection Directive in subtly different ways. For example, Finland requires that, at checkout, supermarkets disassociate the list of items purchased by a consumer from credit card or other personal details and record only the total purchase value—a restriction that does not exist in the UK.

Electronic Commerce Directive

This directive regulates the fast checkout process supported by RFID points of sale with several provisions regarding contractual terms and conditions and dictates that explicit consumer consent be given at all stages. Although exceptions apply to cases in which the interaction medium does not allow for information-rich interactions, RFID's predominantly silent operation stresses this requirement to its limit.

Privacy and Electronic Communications Directive

This directive extends the Data Protection Directive to apply to the recording and use of location data. It also specifies that direct marketing communications are only allowed when the recipient has agreed to be contacted in advance or in the context of an existing customer relationship, in which case companies can continue to market their own similar products on an opt-out basis.

electromagnetic attack—for example, when tags are physically retrieved after disposal by the consumer at home. Disabling the tag is also a significant disincentive for businesses because they can no longer access RFID data, which limits marketing opportunities.

More recently, some have proposed modifying the EPC protocol to include compliance with the EU Data Protection Directive's collection limitation and purpose specification principles.[8] The protocol currently relies on the reader to only collect data relevant to the application at hand. The proposed extensions do not provide a specific solution, but an increasing number of research groups are implementing lightweight encryption algorithms that RFID's very limited computational capabilities can support.[9]

However, key management remains a major challenge for practical deployment. Other research groups have explored schemes for proactive consumer protection—for example, using so-called blocker or cloaking tags—but these devices have limited practicality for the general public.[10]

Even if these or other low-level mechanisms provide the tools necessary to ensure compliance with data protection legislation, they are unlikely to conclusively address consumer concerns because users interact with RFID systems at a much higher conceptual level. Moreover, the expected scale of RFID technology deployment implies that cheap reader devices would be readily available to all, which opens up considerable opportunity for abuse by private individuals.

A final area of concern involves competition among different businesses. Consider, for example, a consumer who enters a supermarket carrying products purchased from a different retailer, or simply RFID-tagged clothing items. Clearly this information could be used for unsolicited commercial communications or collection of personal data, respectively.

RFID AND RISK MANAGEMENT

Many believe that technology and business dominate culture today, yet it is a society's privacy culture that defines its values, sensibilities, and commitments.[11] To be sure, attitudes toward privacy change as technologies emerge that blur the distinctions between what is public and private. Deploying any new technology involves risk, and society relies on experts to accurately assess that risk; failure to do so compromises their role as gatekeepers.[12]

It is thus our profession's responsibility to confront the challenges of RFID in retail. How we deal with these issues will determine the chances of widespread adoption of not only RFID but potentially the whole range of emerging ubiquitous computing technologies. Advising that deployment of RFID, or any technology for that matter, should exploit "consumer apathy" does little to inspire public trust, as does making a tag impossible to remove.

Two aspects of the technology accentuate the trust problem and dictate collaboration across disciplines:

- RFID-based systems' silent and transparent operation; and
- the fact that trust is not a purely cognitive process and thus is not amenable to a strictly quantitative treatment—for example, as a personal utility optimization problem, a popular view within computer science today.

In fact, many of the core challenges involve managing the enormous amounts of data that RFID generates and monitoring the massive increase in points of contact between user and system rather than developing cryptographic algorithms and security mechanisms that control access to tag data.

While individuals' initial entitlement to control their data is well recognized, economic coercion mechanisms based on price discrimination are less so. Such mechanisms result from negotiations between private organizations and public institutions, and this is where our professional social responsibility must play a critical role. Dealing effectively with misuse will become more urgent in the near future.

In the next few years, RFID use in the supply chain will become common at the SKU-level, but item-level tagging will remain restricted to high-value products. Yet, RFID is only one of many sensor technologies that can be used to develop individualized consumer services, which are important in achieving highly accurate differential pricing strategies. As businesses, users, and society in general struggle to cope with this plethora of new data sources and their numerous privacy implications, new mechanisms for commercial use of private data will appear, shopping behavior will change, and consumer activism will increase. ■

References

1. P. Kourouthanassis and G. Roussos, "Developing Consumer-Friendly Pervasive Retail Systems," *IEEE Pervasive Computing*, vol. 2, no 2, 2003, pp. 32-39.
2. R. Want, "The Magic of RFID," *ACM Queue*, vol. 2, no. 7, 2004, pp. 40-48.
3. S. Sarma, D. Brock, and D. Engels, "Radio Frequency Identification and the Electronic Product Code," *IEEE Micro*, vol. 21, no. 6, 2001, pp. 50-54.
4. S.L. Garfinkel, A. Juels, and R. Pappu, "RFID Privacy: An Overview of Problems and Proposed Solutions," *IEEE Security and Privacy*, vol. 3, no. 3, 2005, pp. 34-43.
5. J. Småros and J. Holmström, "Reaching the Consumer through E-Grocery VMI," *Int'l J. Retail & Distribution Management*, vol. 28, no. 2, 2000, pp. 55-61.

6. G. Roussos and T. Moussouri, "Privacy, Security, and Trust in Ubiquitous Commerce," *Personal and Ubiquitous Computing,* vol. 8, no. 6, 2004, pp. 416-429.
7. European Opinion Research Group, *Data Protection,* Special Eurobarometer 196, 2003; http://europa.eu.int/comm/public_opinion/archives/ebs/ebs_196_data_protection.pdf.
8. C. Floerkemeier, R. Schneider, and M. Langheinrich, "Scanning with a Purpose—Supporting the Fair Information Principles in RFID Protocols," *Proc. 2nd Int'l Symp. Ubiquitous Computing Systems,* 2004; www.vs.inf.ethz.ch/res/papers/floerkem2004-rfidprivacy.pdf.
9. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm," *Proc. 6th Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES 2004),* LNCS 3156, Springer-Verlag, 2004, pp. 357-370.
10. A. Juels, R.L. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," *Proc. 10th ACM Conf. Computer and Communications Security,* ACM Press, 2003, pp. 103-111.
11. P. 6, *The Future of Privacy, Volume 1: Private Life and Public Policy,* Demos, 1998.
12. A. Giddens, *The Consequences of Modernity,* Polity Press, 1990.

***George Roussos** is a lecturer in the School of Computer Science and Information Systems at Birkbeck College, University of London. He researches ubiquitous computing, with a focus on the effects of social activity on system architectures and mechanisms to support navigation and findability. Roussos received a PhD in scientific computation from the Imperial College of Science Technology and Medicine, University of London. He is a member of the IEEE, the IEEE Communications and Computer Societies, and the ACM. Contact him at g.roussos@bbk.ac.uk.*