Enabling RFID Retail

George Roussos
Birkbeck College
University of London

The past two years have witnessed an explosion of interest in RFID and supporting technologies primarily due to their rapidly expanding use to track products through the grocery supply chain. Such applications monitor Store-Keeping Units (SKU) rather than individual product items, since item-level tagging is not yet practical due to the relatively high cost of RFID deployment and the very low profit margin of supermarket products. Yet, putting economic and other technical concerns aside, one can easily envision a situation where each item in a supermarket is tagged with an RFID label, shopping carts feature RFID readers and potentially on board computers[1] that recognise products put in the cart, and display information and promotions retrieved wirelessly from the system back-end.

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 use RFID embedded in consumers' loyalty cards to identify individuals. This option could be useful for faster login to the system and to charge the shopping cost directly to the customer account at the point-of-sale (POS). Unless removed at the POS, item level tags will inevitably end up at the consumer home. Without doubt, this scenario opens up numerous privacy concerns.

In this article, I consider different perspectives on RFID retail in the particular context of the European Union and attempt to identify the core issues that must be addressed to enable widely accepted deployment of RFID in retail. The discussion is based on practical experience in building, deploying and evaluating with consumers a system for RFID retail [7].

Item Level Tagging in Retail

One often asked question regards the utility of item level tagging. Although at present there are still considerable technical difficulties and the cost of both tag and reader is too high to make it practical except for high-value products, item-level implementation of RFID has a clear rationale and clear benefits for suppliers and retailers since it is the natural extension of current work on supply chain management. In fact, during the last three decades considerable operational gains have been realised through the implementation of information technology under the so-called Efficient Consumer Response (ECR) initiative. With its aim to maximize value for the consumer and at the same time minimize inefficiencies throughout the supply chain, ECR is also the rationale behind the current interest in RFID.

One of the biggest successes of ECR has been the Vendor Managed Inventory (VMI) approach where 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 data interchange between trading partners, and bar codes offer standardised product identifiers. Use of RFID at the SKU level further improves VMI efficiency by automating the manual scanning of stock and thus provides for continuous and accurate data flows that can be used by enterprise resource-planning (ERP) software and for optimised logistics. An extension of VMI first proposed in the mid-90s [9] is to expand the supply-chain to include the consumer

[1] Alternatively, a mobile device can be used for example the user mobile phone. RFID enabled smart phones are commercially available today and are becoming increasingly popular in Asia.

home: arguably, the replenishment process begins when a product is consumed and it's packaging discarded.

The availability of item-level information can be used for additional purposes, the one of most interest to manufacturers and retailers is user profiling. One cannot underestimate the amount of effort and resources invested every year to attract and retain specific consumer groups with the long-term aim to provide individualised marketing and services[2]. Although direct marketing to the individual is not yet feasible, it is also true that over the past decade there has been rapid progress towards this objective. Notably, a major UK supermarket chain has extended its clustering of customers from 8 to 150 target groups using information collected via their loyalty club scheme and provides different campaigns to address the needs of each particular group. Use of RFID is expected to provide considerable new insight in shopping habits and consumption patterns and those organisations that can best use this information are expected to have a significant competitive advantage. Perhaps a measure of how important is this new information, is the fact that in the past year all major ERP providers have announced support of item-level recording in their products.

In particular, use of RFID in the store as outlined above, creates an information trail that combines location recordings, routes through the supermarket and interactions with products. This data can be aggregated and mined for patterns and consumer routines. Such aggregates can be used to help consumers navigate the store (a particularly important feature for mega-stores) and to develop individualised offers and promotions. For example, awareness of the cart content correlated to individual demographics and life-style choices can be used as the basis for recommendations of specific products, for example food appropriate to a low cholesterol diet, at a suitable price level. Of particular interest is after sales product traceability, which is particularly important for drug anti-counterfeiting, medication compliance, and food monitoring and recall.

Item level RFID infrastructures can be also utilized to develop a variety of useful applications not directly related to supply chain management. For example M&S, a major UK high-street retailer, has implemented item level tagging of men's suits with a view to validate a business case based on more efficient stock control.[3] Current practice is that stock levels, and thus replenishment strategies, are estimated using POS data that frequently result to 8-12% error, especially for retailers of fast moving consumer goods (FMCG). In this case, more accurate estimates result in improved product availability and thus increased sales. Other applications put more emphasis on the consumer experience, for example checking availability of specific sizes and colours of women's shoes at Takashimaya Department Stores in Tokyo and micro-payment services using the Oyster and the Suica cards (in London and Tokyo respectively).

Although tag removal at the POS does not currently impact this application, it is also true that often after a technology is deployed new uses are discovered that may affect consumer privacy. This has already occurred at least once with RFID in the case of active tags used in toll systems: in Florida, USA, the EZ-pass system is used for toll collection and has been re-engineered to record transit speeds of individual cars so as to help in traffic management thus raising considerable privacy risks due to the recording of car locations.

The European Regulatory Environment

The European Union was established as a loose partnership of countries aiming to promote economic co-operation as a means to create safety and prosperity in the region. More recently,

[2] An objective often refereed to as *mass customisation*.

[3] M&S employs RFID tags that do not comply with the EPCglobal standard since the company operates a closed supply chain.

the EU has been taking a more central role in establishing common policies guided by the Charter of Fundamental Rights (2000/C364/01) which outlines the whole range of civil, political, economic and social rights of European citizens and all persons resident. In particular, Article 7 sets out the freedoms of the individual and explicitly refers to the right of “respect for private and family life: right to privacy, home and correspondence”.[4]

While the charter is a set of guiding principles with restricted legal practicality, there are several directives[5] that directly impact RFID retail. In particular, the Data Protection Directive of 1995 (95/46/EC) outlines principles on 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 principles require that data can be collected only for specified lawful purposes and cannot be further processed beyond the scope of collection; data should be adequate, relevant and not excessive in relation to the purpose of collection; data should be kept accurate; data should not be kept for longer than is necessary; that appropriate technical and organisational measures must be taken against unauthorised or unlawful processing; and finally that data should not be transferred outside the European Economic Area unless a similar level of protection is ensured. Further requirements are made regarding the use of sensitive personal data including that related to religion or sexual preferences.

It should be noted that the directive has been interpreted in subtly different ways by different member states. For example, in the case of supermarkets Finland requires that at checkout the list of items purchased by a consumer is disassociated from their credit card (or other personal) details and only the total value of purchase recorded something that is not necessary in the UK for example.

A second directive directly applicable to RFID systems is the Privacy and Electronic Communications Directive of 2002 (2002/58/EC). This directive extends the provision of the Data Protection Directive to apply to the recording and use of location data. It also specifies that direct marketing communications are only allowed in case the recipient has accepted to be contacted in advance or in the context of an existing customer relationship, where companies may continue to market their own similar products on an 'opt-out' basis.

Finally, the fast checkout process supported by RFID POSs is regulated by the Electronic Commerce Directive of 2000 (2000/31/EC) which makes several provisions regarding information of the contractual terms and conditions, and dictates that explicit consumer consent is given at all stages. Although some concessions are made in cases where the interaction medium does not allow for information-rich interactions, RFID checkout stresses this requirement to its limit with its predominately silent operation.

Consumer Perceptions of Privacy in RFID Retail

Recently, we carried out extensive qualitative and quantitative research with a prototype item level RFID retail system [8]. Study participants unanimously objected to any type of RFID recording or to the delivery of personalised commercial communications at home. Both activities were seen as a direct violation of privacy, in which case control of ones immediate environment was seen as more important over access to commercial opportunities.

Consumers were able to identify the implications of the tradeoffs between advanced functionality and privacy protection, which was understood as a core element of system design. However, this does not imply that consumers would accept the uncontrolled use of personal data --- an aspect

[4] It has been often argued that privacy in this case is defined rather narrowly to refer only to the home environment. Even so, this right would be clearly violated if RFID data is collected from consumer homes.

[5] The EU publishes directives that are subsequently implemented as national law by member states.

of the system that attracted significant criticism --- since consumers understood that once collected, the data could be used proactively by the business, in ways that may not be directly related to the provision of the service. In fact, the vast majority of the participants would resist providing their data unless they could be confident that they would be used fairly and only in the context of this particular service. Although they could see the benefit of such a system to business through cost reduction and more accurate prediction of the success of particular offers and promotions, they did not perceive the service as equally or at least as comparably valuable to the consumer.

The practice of using personal data beyond the scope of their collection, appears to violate the trust relationship between buyer and seller and the (silent or explicit) expectation of the consumer that both parties involved would do whatever possible to protect the relationship from outsiders. It is worth relating this finding to recent studies in the UK that have found only 12 per cent of consumers trusting retailers to comply with their Data Protection obligations and that consumers expected law to be their main guarantee against exploitation [1].[6]

Moreover, the existence of a personal profile maintained by a business and the ability to infer facts, habits and routines about an individual was seen as undesirable. Personalisation of the shopping experience during a supermarket visit in the sense of prediction of personal likes and dislikes and shopping habits, was seen as intrusive rather than helpful. Moreover, several participants identified two undesirable aspects of such systems: first, their disruptive effect on established social practice and etiquette, for example roles within the family and perceptions of polite behaviour. Second, the use of such systems by business to further reduce consumer control on shopping decisions and the transformation of the shopping experience to a primarily mechanistic activity. Taking the automation theme to its limit, prediction of free choices was considered to directly challenge ones perception of oneself as a unique person and an individual, free to make his own choices and self-determine.

Several other issues were raised including the desire t have direct control over system operation and the option to allow anonymous use. Finally, questions were raised regarding the restriction of shopping only via this mode and the limitation of choice and the financial safety guarantees available to the user.

Privacy Protection Technologies

A recent attempt to address privacy concerns has been 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 clearly a step towards the right direction, it has limited benefits since consumers still have no practical way of verifying 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 more often implemented in software and cannot withstand a hardware attack, for example when tags are physically retrieved after being disposed of by the consumer at home. It is also worth pointing out that disabling the tag is a significant disincentive for businesses since they can no longer access RFID data, which limits opportunities to effective marketing.

More recently, further modifications to the EPC protocol were proposed [5] to address compliance with the Data Protection Directive, in particular to address the collection limitation and purpose specification principles. The protocol relies on the reader to only collect data that are relevant to the application at hand. These extensions do not address the security principle but

[6] For a complete survey of citizen attitudes on privacy and data processing across Europe refer to [eurobarometer].

an increasing number of research groups are implemented lightweight encryption algorithms, which can be supported by the very limited computational capabilities of RFID [4]. However, the complex issue of key management remains a major challenge for practical deployment. Other groups have explored schemes for proactive consumer protection (for example using the so-called blocker or cloaking tags) but such devices have limited practicality for the general public.

While such low level mechanisms provide the tools necessary to ensure compliance with data protection legislation, they are unlikely to conclusively address consumer concerns since users interact with systems at a much higher level. Moreover, the expected scale of RFID technology deployment implies that cheap reader devices would be readily available to all, a fact that opens up considerable opportunity for abuse by private individuals. A final area of concern is competition between different businesses, for example consider the case of a consumer entering a supermarket carrying products purchased from a different retailer, or simply RFID tagged items of clothing. Clearly this information can be used for unsolicited commercial communications or collection of personal data respectively.

Modernist Culture and the Management of Risk

Technology and business are seen by many as dominant factors over culture. Yet, it is a society's privacy culture and the culture of the material environment that defines our values, sensibilities and commitments [1]. To be sure, privacy is not a static concept but develops slowly as a process of negotiation of the line between the personal and the public. To the consumer, technology implementation is a risk management exercise. In fact, managing risk is a core function of modern society [6] and in doing so societies depend on their trust to experts. Experts take risks on behalf of society and are responsible to realise the full extent of a particular set of dangers and the risks associated with a particular technology. Failure to do so compromises the very idea of expertise and their ability to act on behalf of the public [6].

It is thus the responsibility of our profession to confront and address the particular challenges created by RFID retail. How we deal with these issues will determine public perception of not only RFID but potentially of the whole range of emerging ubiquitous computing technologies and their chances of wider adoption. Advising that deployment of RFID, or any technology for that matter, should exploit "consumer apathy" does little to develop public trust [2] as does making a tag impossible to remove.

In dealing with RFID retail and RFID-based systems in general it is necessary to adopt a holistic approach that addresses different levels of abstraction. Two aspects of this technology accentuate the trust problem and dictate that collaboration across disciplines is required: the silent and transparent to the end user operation of RFID systems; 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 optimisation problem, a popular view within computer science. In fact, many of the core challenges have more to do with the management of the enormous amounts of data generated by RFID and the massive increase in the number of points of contact between user and system, rather than the minutiae of crypto algorithms and security mechanisms controlling access to the data contained in a tag.

Finally, while the initial entitlement of individuals to control their data is relatively well recognised, the economic mechanisms of coercion based on price discrimination are less so. Such mechanisms are mediated via the identities of the organisations and public institutions and this is where our professional social responsibility has to play a critical role. Dealing effectively with such misuse will become more urgent in the next few years.

Conclusions

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 a variety of sensor technologies that can be used to develop individualised consumer services, which are important in achieving high accuracy of differential pricing strategies. While businesses, individuals and societies alike struggle to cope with this plethora of new data sources and their numerous implications for privacy, new mechanisms for commercial use of private data will be introduced; the learnt behaviour of shopping will change; and consumer activism will increase.

References

[1] P. 6. *The Future of Privacy. Volume 1: Private Life and Public Policy*. Demos Think Tank, London, UK, 1998.

[2] H. Dunne. *Message Development*. Auto-ID Sponsor briefing, June 2002.

[3] Eurobarometer. *European Union Citizens' Views about Privacy*. Special Eurobarometer 196, 2003.

[4] M. Feldhofer, S. Dominikus, J. Wolkerstorfer. "Strong Authentication for RFID Systems using the AES Algorithm", *Proc. of CHES 2004*, Boston, USA, August 11-13, 2004.

[5] C. Floerkemeier, R. Schneider and M. Langheinrich. "Scanning with a Purpose – Supporting the Fair Information Principles in RFID protocols", *2nd International Symposium on Ubiquitous Computing Systems* (UCS 2004), Tokyo, Japan, November 2004.

[6] A. Giddens. *The Consequences of Modernity*. Cambridge: Polity Press, 1990.

[7] P. Kourouthanassis and G. Roussos. "Developing Consumer-Friendly Pervasive Retail Systems", *IEEE Pervasive Computing*, Vol. 2, No 2, pp. 32- 39, 2003.

[8] G. Roussos and T. Moussouri. "Privacy, security and trust in ubiquitous commerce", *Personal and Ubiquitous Computing*, Vol. 8, No. 6, pp. 416 – 429, 2004.

[9] J. Smaros and J. Holmstrom. "Reaching the consumer through e-grocery VMI", *International Journal of Retail & Distribution Management*, Vol. 28, No. 2, pp. 55-61, 2000.

SIDEBAR: RFID OPERATING PRINCIPLES

Radio Frequency Identification, or RFID as it is most commonly known, is a generic term used to refer to any system that can transmit identification numbers over radio. For this reason, this single term is used for a wide variety of technologies and systems, a fact that often makes understanding of and talking about RFID difficult. In fact, RFID systems have been around for at least 40 years with their first use by the military in the Friend-or-Foe application introduced shortly after the Second World War, to automatically identify friendly and enemy aircraft from a distance. Since then, they have been used in a variety of applications, notably in animal tracking, automatic toll collection, car immobilisers and building access control systems [3].

Yet, the past few years have witnessed a rapid growth in public interest for such systems due to a variety of high profile deployments that directly affect individuals in their everyday activities [2]. Supermarkets and retailers across the world are planning item-level large scale deployments in consumer goods that will leave very few citizens in developed societies unaffected. Such implementations have found champions in every continent: Wal-Mart in the US, Marks & Spencer and Tesco in the UK, Metro in Germany, Coles Myer in Australia and Mitsukoshi in Japan are all leading retailers that are currently implementing RFID solutions across their supply chain. Moreover, governments are planning the use of RFID (which would include biometric information including images and iris scans) embedded into passports to improve security under a world-wide initiative led by the US. RFID has been transformed from an arcane business technology into an everyday-personal technology that affects all.

RFID systems have two parts: the reader and the tag. An RFID tag is made up of a microcontroller, an antenna (either wire or printed using conductive carbon ink) and glass of polymer encapsulating material that wraps around the antenna and processor. The identification process is initiated by the reader which generates an RF field (at a specific frequency defined for the particular system) thus causing a voltage difference at the tag antenna endpoints via inductive or capacitive coupling. The tag detects this and responds by transmitting the identifier that it holds, after an optional step which authenticates the reader as a valid recipient of the identifier via a challenge-response mechanism.

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. On the positive side, they do not require a power source, passive RFID tags continue to operate until damaged or discarded. However, this comes at a cost as in normal operating circumstances they can be read only when the reader is within a few centimetres and the data transmitted have a high error rate. Active RFID tags on the other hand have a much longer range which can be more than 100 metres, they provide more reliable communication but they expire after a period of use when their battery runs out (this can be as high as 7 years in some systems). Because they incorporate a battery, active RFID tags have significantly larger size than passive tags. In either case, the actual transmission range of a tag depends on the size of the antenna: a larger antenna provides a longer reading range.

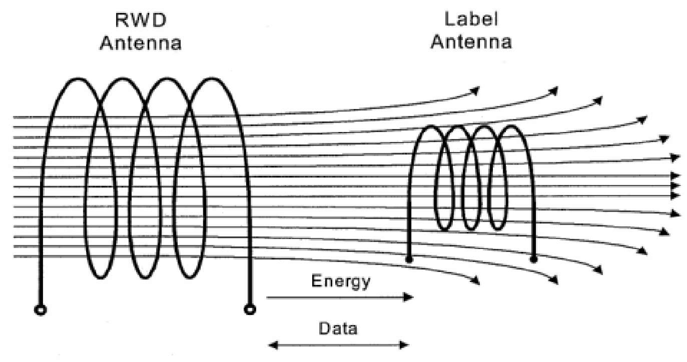

Figure 1. RFID operation: The reader antenna provides the power for the tag to transmit its stored identification number.

The frequency at which an RFID system operates has considerable implications for its actual performance. RFID-based security cards for example often operate between 125 and 134 Khz, where reading ranges are short but where the RF signal is not significantly absorbed by water (a critical issue in this case, since the human body is made up mostly of water). Modern systems designed for use in supermarkets operate in the 800Mhz (Europe) or 900Mhz (US) range, offering longer reach and considerably higher data rates which are required to offer the required functionality i.e. 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 with the result that even a few items placed in a shopping cart, e.g. soda cans, can prevent the accurate recording of products, thus making the quick checkout concept unworkable [1].

Perhaps the most important implication of RFID technology today is due to its use within bigger information systems on the internet: the identifiers retrieved from a tag can be used to query (or update) online databases that hold information about object and people alike. For example, given an Electronic Product Code retrieved from a supermarket product, the Object Naming Service directory will locate and retrieve information about this product published by the manufacturer via the EPC Information Service -- much in the same way that the Domain Name System provides information about individual hosts on the internet. This information will relate to the particular item rather than the product class it belongs to, as is the case with bar codes in common use today. This ability to silently retrieve and record product or personal identifiers combined with the advanced, real-time information processing capability available today, are the main factors that have increased the sense of uneasiness about the use of RFID.

Sidebar References:

1. S. Garfinkel, A. Juels and R., Pappu, "RFID Privacy: An Overview of Problems and Proposed Solutions," *IEEE Security and Privacy*, vol. 3, no. 3, pp. 34-43, 2005.
2. S. Sarma, D. Brock and D. Engels, “Radio Frequency Identification and the Electronic Product Code,” *IEEE Micro*, vol. 21, no. 6, pp. 50-54, 2001.
3. R. Want, “The Magic of RFID,” *ACM Queue*, vol. 2, no. 7, pp., 2004.