12-31-2007

Assessing the Impact of Privacy-Enhancing Technologies for RFID in the Retail Industry

Frederic Thiesse
University of St. Gallen

Christian Floerkemeier
ETH Zurich

E. Fleisch
University of St.Gallen

C. Sorensen
University of St.Gallen

ASSESSING THE IMPACT OF PRIVACY-ENHANCING TECHNOLOGIES FOR RFID IN THE RETAIL INDUSTRY

Frédéric Thiesse
ITEM-HSG, University of St. Gallen
frederic.thiesse@unisg.ch

Christian Floerkemeier
Auto-ID Labs, MIT
floerkem@mit.edu

Elgar Fleisch
ITEM-HSG, University of St. Gallen & D-MTEC, ETH Zurich
elgar.fleisch@unisg.ch

Abstract

The perpetual debate on RFID as a risk to privacy has lead to a variety of technical proposals for securing RFID data and encompasses, apart from general IT security measures, a number of RFID-specific "Privacy-Enhancing Technologies (PETs)". Against the background of an imminent obligation to include privacy-enhancing mechanisms in the retail industry's current RFID deployments, this contribution provides a critical review of the undesired side-effects of PETs on information systems and business processes. As our investigation shows, the practical impact includes increased hardware costs, reduced capabilities of the technology, and a range of process-related issues, e.g. in the context of password management and consumer benefits. We discuss the managerial implications for RFID implementation strategies and propose a set of alternative starting points for fostering the public acceptance of the technology.

Keywords: Radio Frequency Identification (RFID), Retail, Privacy-Enhancing Technologies.

Introduction

Practical relevance of the contribution

The technologies of Radio Frequency Identification (RFID) enjoy an enormous interest at the current time, not only from the standpoint of research but also from corporate practice. Enterprises from diverse branches are hoping for solutions to a wide range of management problems through RFID, from simple increases in processing efficiency for the receipt and despatch of goods in distribution centres through to improvements in goods availability on the shelves and on to the struggle against shrinkage and product counterfeiting. However, over the past few years, concerns about the possible risks of using RFID have increasingly been voiced.

The risks associated with RFID that are discussed in the public include both the direct impact of electromagnetic radiation on health, as well as indirect economic consequences such as the elimination of jobs through increasing automation (Duce 2003). The most frequently voiced fear refers to the misuse of data generated by RFID, resulting in an undesirable intrusion into the privacy of individuals. Here, the fears of the general public extend from the analysis and evaluation of individual consumer behaviour to an omnipresent surveillance through the "privacy snatchers" (Bibby 2006) in the form of transponder labels. The debate has become additionally heated through the actions and campaigns of pressure groups such as the American Association "Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN)" and similar European organisations. For example, the well-publicised "Big Brother Award" given to the Metro Group, along with a demonstration on the 28th of February 2004 in front of the Metro Future Store in Rheinberg, caused them to ultimately withdraw the RFID-based customer cards that were in circulation at the time (Albrecht and McIntyre 2005). Further examples in Europe and the US, such as CASPIAN's call for a boycott of Gillette products because of tests with RFID transponders in razor blade packages, show that these are not isolated incidents.

On the level of European policy-making, the debate has so far culminated in an online consultation conducted by the European Commission between July and September 2006. 2190 respondents answered questions about RFID use, privacy, standardisation, frequency spectrum, and other related issues. One of the interesting results of the survey was that about two-thirds of all respondents had the opinion that the best solution to eliminate or greatly reduce the concerns of security, data protection and privacy, which may arise from deploying applications of RFID technology, are the development of technical solutions allowing to disable RFID tags and/or awareness raising campaigns to educate consumers. Almost half of all respondents had the opinion that “Privacy-Enhancing Technologies (PETs)” should be made mandatory in RFID applications. 61 % of the respondents had the opinion that a RFID tag related to a product in a supermarket should be automatically de-activated at the point of sale. A removable sticker attached to the product itself and a so-called “proximity tag” with a very short reading distance were advocated by 46 % and 40 % of all respondents, respectively (EU 2006).

Research question and structure

Against the background of an imminent obligation to implement privacy-enhancing mechanisms, this contribution investigates the practical impact of PETs on the retail industry’s current RFID deployments. In contrast to previous works, we do not aim at evaluating the benefits for consumer privacy but rather the undesired side-effects of PETs on information systems and business processes. For this purpose, the remainder of the paper is organised as follows: First, we provide a short overview of RFID technology and privacy issues. Second, we present a review of the existing body of literature on PETs. In the following, we analyse the potential impact of PETs on processes in the retail supply chain. We then discuss the managerial implications that can be drawn from our findings. The paper closes with a summary and an outlook on further research.

Background

Radio Frequency Identification

RFID is a technology for the automatic identification of physical objects by radio such as industrial containers, palettes, individual products and also people. The identification event takes place over transponders located in or on the respective objects, which can be addressed without physical contact, over the so-called "air interface", by the antenna on a scanner device. Typical areas of application for RFID lie, adjacent to classics such as animal identification or access control systems, above all in Supply Chain Management, where the technology makes possible simplified goods turnover, automatic stock control in the storeroom resp. on the sales floor, theft protection, product tracking etc. (Bose and Pal 2005).

The reason for the recent rapid and escalating use of RFID lies primarily in advanced miniaturisation, maturity as well as in the constant price decline which makes the use of RFID economically viable in ever more areas of application (Sarma 2001, Want 2004). Another trigger has been especially the activities of the Auto-ID Center, a project founded in 1999 at the Massachusetts Institute of Technology (MIT), in cooperation with numerous industrial sponsors, for the development of RFID Standards. The main result of the Auto-ID Center was the "Electronic Product Code (EPC)" (Sarma 2005), a worldwide unambiguous numbering scheme for the designation of arbitrary physical goods which should ensure the interoperability of the technology in supply chain wide applications. Since the termination of the Auto-ID Center in October 2003 the EPC technology is being commercialised and further developed by EPCglobal Inc., a subsidiary of GS1, the industry organisation responsible for Barcode standardisation (Sarma 2005). In the following years, EPC became the technical foundation for the multiple RFID initiatives of large chain stores such as Wal-Mart and Metro, and also for industrial enterprises such as Novartis or the US Department of Defense.

RFID as a threat to privacy

The threat to privacy through the use of information technology has its origins in the ability to permanently save and link information about individuals (Culnan and Bies 2003, Perrin 2005, Spinello 1998). With RFID and similar technologies, yet another dimension to data acquisition has developed through (a) the temporal and spatial extension of data collection activities, (b) the inability to recognise and reconstruct data collection, (c) the acquisition of new data types through real-time monitoring, (d) the ever decreasing transparency of reasons for acquiring data, and (e) the uncontrolled data access caused by extreme interconnectedness (Cas 2004, Langheinrich 2005). Thus, the use of ID tags, sensors and location systems leads to the disappearance of what Lessig (1999) calls "structural" or "architectural" barriers, i.e. economic factors that make privacy intrusions costly or unprofitable.

In the case of RFID, the privacy-related problem arises particularly because of the globally unique identity of each good and the possible linkage with the owner. That facilitates, in principle, an automatic tracking of individual people (Juels 2005, Sarma et al. 2002). Weinberg (2005) differentiates between the following three privacy risks from RFID: First, RFID may allow for robust and pervasive profiling, incorporating data from personal belongings and documents that is added to an individual's profile. Second, RFID can be used to locate objects and people in space, thus enabling automatic surveillance of an individual's activities. Third, after reading RFID tag information, people or devices associated with the reader network can take actions based on their knowledge of an individual's objects and profile. Even if the listener can't make a connection between RFID data and personally identifying information, the action threat remains, e.g. in the form of price discrimination, the practice of charging each customer the maximum amount he or she is prepared to pay (Odlyzko 2003, Stajano 2005).

Literature Review

Privacy-Enhancing Technologies for RFID

The perpetual privacy debate has lead to a variety of technical proposals for securing RFID data and encompasses, apart from general IT security measures, a number of RFID-specific PETs. These prevent the uncontrolled reading of transponders, the manipulation of information saved in them as well as eavesdropping, i.e. the interception of data transmissions between transponders and readers. The following enumeration provides an overview and a classification of the approaches proposed in academic literature and standard specifications:

- *Physical shielding.* The simplest protection from access to transponders by third parties is physical separation by means of a metal net or a foil sheet according to a Faraday Cage **(Kumar 2003)**. Various examples of this PET have been commercialised in the form of so-called "RFID foiling kits" and "RFID protection cases", e.g. by privacy activist groups such as the German "Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V (FoeBuD)" (Association for the Promotion of Public Mobile and Immobile Data Traffic). While physical shielding is a simple form of protection for RFID-equipped passports and other small items, it is evidently unsuitable for most other products such as clothing, watches etc.
- *Physical destruction.* An easy way of protecting consumers from RFID misuse is to remove or to destroy the transponder after purchase. For this purpose, **Karjoth and Moskowitz (2005)** propose the use of "clipped tags" that permit the customer to disable a tag by mechanically altering it. Possible realisations of clipped tags include tags with removable electrical conductors (e.g. conductors made of scratch-off material), perforations that separate the antenna from the microchip, and tags whose antenna is affixed to a removable peel-off layer. In contrast to electronic PETs, clipped tags provide immediate visual confirmation that the tag has been deactivated.
- *Blocking.* Another means to prevent any communication between transponders and readers in reach is the use of jammer transmitters **(Kumar 2003)** that completely block a particular frequency band. A more sophisticated procedure is the use of "blocker tags" proposed by **Juels et al. (2003)**, i.e. tags that positively respond to any request from a reader device. Thus, blocker tags circumvent the reader's anti-collision protocol and keep it from identifying transponders in its environment. Furthermore, the authors suggest to implement a programmable "privacy bit" in transponders that allows for distinguishing between private tags that are protected by the blocker tag, and public tags that are accessable anytime. "Soft blocking" **(Juels and Brainard 2004)** is an alternative, lightweight approach that bases on blocker tags that resemble ordinary RFID tags whose only special distinction is a special tag identifier. In soft blocking, a reader would begin a scan by checking for tags with this identifier and refrains from scanning if it finds one. It is understood that soft blocking relies on RFID readers that are equipped with blocker-compliant firmware.
- *Proxying.* The concept of proxying relies on privacy-enforcing devices carried by consumers in the form of distinctive items or integrated into mobile phones. **Floerkemeier, Schneider and Langheinrich (2004)** propose a prototype "Watchdog Tag" that monitors RFID scanning operations and collects information from readers, e.g. on their privacy policies. The device does not keep the readers from accessing tags but rather records information on tag access operations. **Rieback, Crisp, and Tanenbaum (2005)** propose a similar device, called "RFID Guardian". The Guardian acts as a RFID

firewall that implements various privacy policies and intermediates reader requests to tags. Tags that the user wants to hide from readers are selectively jammed.

- *Tag anonymisation.* Various concepts have been developed for anonymising tags after purchase in order to prevent tracking of items by third parties beyond the point of sale. **Sarma et al. (2002)** propose the idea of effacing unique identifiers in tags to address the tracking problem, but retaining product-type identifiers (i.e. traditional barcode data) for later use. **Inoue and Yasuura (2003)** suggest that consumers be equipped to relabel tags with new identifiers, but that old tag identifiers remain subject to re-activation for later public uses. **Weis et al. (2003)** present a cryptography-based approach that can be used to lock the tag. In this scenario, a hash function generates a new ID code for the tag using a random key, which is also necessary to unlock the tag. As with the other previous concepts, hash-based access control does not prevent the tracking threat since the tag still sends a static ID upon request. For this reason, the authors also propose a more complex algorithm that requires tags with random generators: Tags respond to reader queries by generating a random value *r*, then hashing its ID concatenated with *r*, and sending both values to the reader. A legitimate reader identifies one of its tags by performing a brute-force search of its known IDs, hashing each of them concatenated with *r* until it finds a match. Although impractical for retailers, this mode is feasible for owners of a relatively small number of tags. **Juels (2004)** proposes another approach with changing tag IDs that requires less logic on the tag. Instead of generating ID codes, each tag has a set of pseudonyms p_1, p_2, … p_k that the tag is cycling through each time it's read. The tag's owner 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, e.g. a tag might release a new pseudonym only every five minutes. **Juels and Pappu (2003)** propose a re-encryption concept specifically designed for banknotes. In their scheme, banknote tag serial numbers are encrypted with a law-enforcement public key. The resulting ciphertexts undergo periodic re-encryption to render multiple appearances of a given RFID tag unlinkable. Because of the severely restricted computing resources of RFID tags, they propose that re-encryption be performed by external computing agents, for example, publicly provided privacy-enhancing stations in stores. **Feldhofer et al. (2004)** propose an authentication mechanism based on a simple two-way challenge-response algorithm, i.e. symmetric key encryption. The problem with this approach is that it requires to have AES implemented in an RFID tag.
- *Tag deactivation.* In contrast to physical destruction, some authors have proposed mechanisms for deactivating the transponder IC permanently or temporarily. The best-known example of this category of PETs is the so-called "kill command" as it was specified in EPCglobals's "EPC Class 1 Generation 2 (EPC Gen2)" standard **(EPCglobal 2005)**. Gen2 Tags deactivate themselves upon receiving the kill command code which must be accompanied by a 32 bit security code. In order to avoid the disadvantages of tag deactivation, **Spiekermann and Berthold (2004)** propose a password-based model. In their scheme, the user puts the tag into sleep by sending a disable command and a password which could be automatically generated at the point of sale and printed on the customer's receipt. In the following, the tag does not respond to reader queries anymore until it receives the corresponding enable command and the right password. **Engberg et al. (2004)** suggest a similar, but more complex algorithm: Their "zero knowledge authentication" approach is based on a shared key that is necessary to access the tag. The tag does not require a random generator, but it has to store the timestamp of the last query; furthermore, all reader devices must be synchronized.
- *Bug-safe RF protocols.* A further PET category sets the focus on eavesdropping attacks. This attack model makes use of the fact that legitimate readers must operate at power levels that not only transmit information (i.e., commands) to the tags, but also supply enough energy to the tag to process and reply these commands. Thus, a third party might simply overhear the signals being sent back from a tag to a legitimate reader, without itself having to be close (or powerful) enough to actually power the tag. Against this background, **Weis et al. (2003)** propose a secure anti-collision protocol which guarantees that readers never transmit entire ID codes during the tag singulation phase. Based on the works by **Rivest (1998)**, the authors also suggest a second procedure based on broadcasting of "chaff" commands, i.e. commands from the reader, intended to confuse or dilute information collected by eavesdroppers. By negotiating a shared secret, these commands could be filtered by tags. In order to keep distant readers from accessing tags, **Fishkin and Roy (2003)** propose an antenna-energy analysis procedure. In this scenario, tags measure the signal-to-noise ratio of the data received from a reader which gives a rough indication of read distance. When apparently scanned at a distance, tags might either release partial information or refuse to respond to queries.

Summary of side-effects

RFID components for use in the retail supply chain have been optimized for low cost, long range, and high identification speeds. Tags should ideally cost a few cents only, have a range of a few meters, and hundreds of tags should be identified per second (Sarma 2005). However, the PET concepts presented in the previous subsection impact these performance indicators (cf. Table 1):

- *Identification speed.* To reduce the overall cost of an RFID system, RFID tags used in retail logistics operate without a battery. The RFID tags are powered by the electric and/or magnetic field generated by the RFID reader. The result is that these "passive" RFID tags frequently loose power as they are moving past a reader. To address this characteristic of long range, passive RFID systems, RFID communication protocols, such as EPC Gen2, use very short data packets during the identification phase. This permits the successful identification of the tags even when they are only powered for a few hundred microseconds. In contrast to that, at low clock frequencies as can be found on RFID transponders, the AES encryption of a single 128 bit string, for instance, would take as long as ten milliseconds (Feldhofer et al. 2004). Cryptography-based PETs that rely on the exchange of long data packets and time-intensive computations will thus result in significantly reduced identification speeds. The same holds to a smaller extent for the use of proxies due to the additional overhead required for communication between the proxy device and the RFID reader.
- *Read/write range.* Due to the low signal-to-noise ratio characteristic for long range RFID systems, there is also the disadvantage that long data packets are more likely to be corrupted by transmission errors. In a worst case scenario, tags might not be identified at all, e.g. as they move collectively past an RFID reader on a conveyor belt. The PETs using cryptographic function also require additional power to carry out the computations. While there are some very low power implementations available (e.g. Feldhofer et al. 2004), these still require as much power even at low clock frequencies of 100 kHz as the overall power consumption of a standard UHF RFID chip (Karthaus and Fischer 2003). The maximum operating range is thus significantly reduced.
- *Chip cost.* To decrease the RFID tag cost even further, the microchip of the RFID tag should be as small as possible to reduce semiconductor manufacturing costs (Sarma 2001). Cryptographic functions implemented on the RFID microchip to increase the silicon footprint, however. Even the tiny AES implementation by Feldhofer et al. (2004) requires an additional 3400 gates. This corresponds roughly to 20% increase in chip area of a conventional UHF microchip (Glidden 2004) and thus to a 20% increase in semiconductor manufacturing cost.
- *Label cost.* The cost of the RFID tag does not only depend on the microchip cost, but also on the tag antenna cost and the cost of attaching the tag to the product. Additional antenna features such as the perforation needed to physically disable the tag as proposed by Karjoth and Moskowitz (2005) will thus increase the antenna manufacturing cost. This kind of "clipped" tags can also no longer be embedded in conventional packagings, which would increase the integration cost even further.
- *Tag functionality.* Some PET schemes not only prevent undesired data collection by third parties but rather render impossible other applications as well by deleting parts of the tag's memory or by permanently deactivating the tag entirely. The same problem can arise in the case of blocking or proxying devices that prevent any access to the tag regardless of its purpose.
- *Key management.* Schemes that rely on secret passwords or codes stored on the RFID tags, e.g. to authenticate a kill command, lead to significant system integration costs. A large retailer would need to keep a database with an individual password for each retail item sold to prevent the mass killing of RFID tags that carry a common password. Since the tags are attached to the products by the manufacturer and not the retailer, who has to eventually disable the tag, any of the password-based PETs mandate significant efforts for data exchange among supply chain partners.
- *Device cost.* Shielding, blocking, proxying, and password-based approaches that require an additional device to safeguard the privacy of the individual also lead to increased hardware cost. However, these additional devices will not necessarily be provided by the retailers, but privacy-concerned individuals will have to purchase the devices themselves. Additional cost is also to be expected for RFID readers that implement more complex protocols and privacy policies.

Impact analysis

The current use of RFID in the retail supply chain is most of all focused on the tagging of logistical units, i.e. pallets and cases, but some first examples of RFID-equipped sales units can be found as well (apparel, cosmetics, drugs etc.). Since privacy-related issues only arise in the latter case, we restrict ourselves to a consideration of the relevant business processes with item-level tagging. Detailed depictions of RFID applications in retail were given e.g. by Agarval (2001), Chappell et al. (2002), Kärkäinnen (2003), Loebbecke (2005), and Tellkamp et al. (2004).

Consumer products are tagged in the manufacturing process itself or at a later stage of the supply chain which allows for the automatic tracking of deliveries to the stores. Depending on the respective structure of the logistical network, a sequence of intermediate transport and warehouse management tasks are conducted by the CPG manufacturer, the retailer, a wholesaler or a logistics service provider. These processes usually comprise a broad range of identification events for inbound and outbound deliveries as well as inventories in distribution centres. Furthermore, RFID is also used in the stores in order to improve shelf replenishment processes and to enable product information kiosks, digital shopping assistants, and faster check-outs at the point of sale. This is also where consumers are first confronted with RFID. If the RFID tag is not removed at the POS, it remains part of the product over its entire life-cycle. This includes everyday usage of the item as well as after-sales services of the retailer or the manufacturer, e.g. maintenance and repair, warranty claims, or product exchange.

Table 1. Negative side-effects of PET concepts on RFID systems: × = categorical, (×) = conditional

		Identification speed	Read/write range	Chip cost	Label cost	Tag functionality	Password management	Device cost
Physical shielding	Kumar 2003					(×)		×
Physical destruction	Karjoth and Moskowitz 2005				×	(×)		
Blocking	Kumar 2003					(×)		×
	Juels et al. 2003					(×)		×
	Juels and Brainard 2004	(×)				(×)		×
Proxying	Floerkemeier et al. 2004	(×)						×
	Riebeck et al. 2005	×						×
Tag anonymisation	Sarma et al. 2002			(×)		×		
	Inoue and Yasuura 2003			(×)			×	(×)
	Weis et al. 2003	×		×			×	(×)
	Juels 2004	(×)		×			×	(×)
	Juels and Pappu 2003	×	×	×			×	(×)
	Feldhofer et al. 2004	×	×	×			×	
Tag deactivation	EPCglobal 2004		×	(×)		×	×	
	Spiekermann and Berthold 2004		×	(×)			×	(×)
	Engberg et al. 2004	×		(×)			×	(×)
Bug-safe RF protocols	Weis et al. 2003	(×)		(×)				
	Rivest 1998	×						
	Fishkin and Roy 2003			×		×		

Table 2 provides an overview of the relevance of PET side-effects to these processes. According to the differing nature of their impacts from an economic perspective, the before-mentioned side-effects can be grouped into the following categories:

- *Technology cost.* The first and most evident consequence of PET side-effects is the higher cost of hardware components owing to the increased complexity of protocols and tag designs. This problem mostly affects semiconductor and label manufacturers whose market is traditionally very price-sensitive which has its root cause in the low margins of most consumer goods. The same applies to a smaller extent to reader manufacturers who would have to implement PET mechanisms in their products as well. Higher hardware costs are eventually shifted on to the CPG manufacturers which influences their and the retailers' ROI calculations depending on the existence of cost sharing agreements.
- *Data quality.* The deterioration of RFID performance indicators (i.e. identification speed and read/write range) leads to higher process costs along the supply chain because of worsened identification rates. Cryptography-based mechanisms, for example, result in an increase in energy demand of the RFID tag which conflicts with existing legal regulations regarding electromagnetic radiation. The read/write range of RFID would thus decrease significantly. European companies would be affected by this in particular since ETSI regulations in the EU are more restrictive than their FCC counterparts in the US (ITU 2005). A similar issue is the achievable read rate which is mostly determined by the technology's identification speed. Under real-world conditions, RFID read rates can reach more than 99% for many product categories, but drop below 30% for goods that contain substantial portions of water or metal (GS1 2005). PET mechanisms, which increase the complexity of RFID protocols in general, further reduce the number of items that can be identified per time unit. Both

effects are eventually reflected in insufficient data quality which partly eliminates the desired process savings and changes cost/benefits ratios of RFID in comparison to the barcode, e.g. because of inventory inaccuracies or undetected shrinkage.

- *System integration.* The management of password data among supply chain partners still poses a widely unsolved problem. PET mechanisms that allow for tag deactivation or anonymisation would have to be secured by keys in the very moment when the tag is attached to the product in order to make sure that tags cannot be deactivated or manipulated by unauthorised third parties. These keys must then be forwarded to all following stages in the supply chain which requires substantial system integration efforts that might even surpass the complexity of today's EDI deployments. On the one hand, this is owing to the sheer mass of password data that would be generated for billions of consumer products. On the other hand, the large number of partners and their interrelations in retail supply chains increase the complexity of interfaces and data exchange formats.
- *Consumer convenience.* PET mechanisms that impact the tag's functionality after purchase have an impact on virtually all after-sales services that rely on unique object identification. As a consequence, most product-related benefits from RFID for the consumer could not be realised. This disadvantage could be avoided by tag anonymisation concepts which allow for reactivating the tag. However, tag anonymisation imposes on consumers to buy and use a personal device for tag communication and key management, i.e. they become responsible for managing privacy on their own. A simpler – but nevertheless troublesome – alternative would be to give customers the opportunity to manually destroy tags or to shield their property using special shopping bags.

Table 2. The economic impact of PET side-effects on retail processes (TC = Technology cost, DQ = Data quality, SI = System integration, CC = Consumer convenience)

	Identification speed	Read/write range	Chip cost	Label cost	Tag functionality	Password management	Device cost
CPG manufacturing			**TC**	**TC**		**SI**	
Transport logistics	**DQ**	**DQ**				**SI**	
Warehouse management	**DQ**	**DQ**				**SI**	
In-store logistics	**DQ**	**DQ**				**SI**	
Check-out	**DQ**	**DQ**				**SI**	**CC**
After-sales services					**CC**	**CC**	**CC**

Discussion

The managerial implications that can be drawn from our analysis are twofold. First, it is evident that the decision to implement a particular PET can have a substantial negative impact on technical capabilities of hardware components, ROI calculations and an organisation's RFID strategy as a whole. Some of the mechanisms described before can immediately be regarded as not viable, because they are simply impractical. This is a result of excessively high technical requirements, significant complexity for the user or for the fact that various RFID applications are rendered impossible in advance. The need for managing passwords, hash values, etc. along the entire supply chain is an additional drawback of many approaches which poses a barrier to rapid adoption. Furthermore, a second aspect that may prove even more important is the question of consumer perceptions of PETs. Most of the solutions pass on to the consumer the organisational effort for privacy protection, similar to an opt-out procedure through the technology. However, the additional security acquired is neither visible nor perceptible and, even worse, reliable verification is impossible. As de Jager (2005) puts it regarding the EPC Kill Command: "Kill technology doesn't work. You can't kill the image of the RFID chip that's in my head. [...] Kill technology is a dead end because it solves the wrong problem. The problem is trust. There is a good way to kill an RFID chip: Throw it in a microwave and wait until you see the sparks. [...] When I *see* the fireworks inside my microwave, I know that tag is dead."

In contrast to other everyday technical safety mechanisms, for example the brakes of a car, which do not presuppose trust, but rather create it, all mentioned PETs that include no physical destruction of the tag do not provide the user with a direct "look & feel" experience (Juels 2006). As Günther and Spiekermann (2005) found from an analysis of consumer perceptions, "regardless of privacy-enhancing technology employed, consumers feel helpless toward the RFID environment, viewing the network as ultimately more powerful than they can ever be". Therefore, despite the clear need for additional and ongoing technological development, the objective of achieving an improved acceptance of technology cannot be achieved through such measures alone.

This view is also supported by several findings from IS research on the acceptance of information and communication technologies. From this perspective, the implementation of RFID-related PETs can be interpreted as an attempt to foster so-called "technology trust", i.e. trust in an IT infrastructure based on technical safeguards and protective measures (Knights et al. 2001, Ratnasingham and Pavlou 2002). Pavlou (2001), for instance, demonstrated that trust influences the perceptions of risk which has a direct impact on intentions to use a particular technology. However, technology trust is only one out of various other antecedents of technology acceptance. The concept of institutional trust, for example, refers to the security one feels about a situation because of guarantees, regulations, safety nets or other structures (Shapiro 1987, McKnight et al. 1998, Gefen et al. 2003), e.g. through self-regulation or the involvement in the official statutory process. Interpersonal trust, again, refers to the relation between the trustor and the the specific other individual (or party) that one trusts (McKnight and Chervany 2002). One option for the development of interpersonal trust is to formulate processes in such a way that customers gain the impression of "procedural fairness", that is, an appropriate handling of business activities (Culnan and Armstrong 1999). Aside from trust concepts, perceptions of long-term usefulness and ease of use of technical artefacts are also known to have a significant influence on the acceptance of new technologies (Davis 1989).

As a consequence, companies involved in RFID deployments should develop privacy strategies beyond the present predominantly technology-oriented perceptive. An open dialogue with customers, for example, plays an important role in gaining or regaining confidence and credibility. Another instrument is the formulation of clear and for all sides obligatory rules, e.g. in the form of EPCglobal's "Guidelines on EPC for Consumer Products". Furthermore, improved processes can increase customer acceptance of technology through additional services and benefits (Eckfeldt, 2005). Various surveys e.g. indicate a readiness by consumers to accept RFID in connection with improved product security, faster checkouts or easier returns (Gartner 2003, CGEY 2004).

Summary and Outlook

The public debate on RFID and privacy is currently moving itself in the classical constellation of enterprises vs. NGOs. In this phase the stakeholders are still in a position to exert influence in how aspects come to fruition, as conflict intensifying or conflict extenuating. Manufacturing and retailing have won some time through the withdrawal from several critical areas of application and the decision not to apply RFID at the individual product level in the first step, but only to logistical units. However, with the further development of the technology and, at the same time, sinking prices, over time a number of applications are likely to become economically viable which entail transponders in individual products that will remain activated beyond purchase.

At this point in time at the latest, RFID suppliers and users will have to deal with the possibilities and drawbacks of PET concepts. As our investigation has shown, their practical impact on retail processes can be severe. Particularly the negative influence on bulk readings and read/write ranges of many proposals could endanger the attractiveness of RFID technology. Increasing cost of hardware components and system integration is a further threat that could easily make the rationale for replacing barcodes with RFID tags obsolete. Not least, the positive impact on consumer perceptions of RFID seems highly questionable. In this regard, it is surprisingly most of all the cheapest and simplest PET concepts (i.e. physical shielding and destruction) that look more promising than the complex ones.

Our contribution could be a starting point for further research in various directions. First, more empirical research will be necessary in order to get a better understanding of public perceptions of RFID and privacy risks. Second, current research on PET concepts should put more emphasis on user acceptance studies and quantifications of their economic impact. A third opportunity could be the development and evaluation of RFID consumer applications in retail environments.

References

Agarwal, V. "Assessing the benefits of Auto-ID Technology in the Consumer Goods Industry," Auto-ID Center, MIT, Cambridge, MA, 2001.

Albrecht, K., McIntyre, L. "Spychips: how major corporations and government plan to track your every move with RFID," Nelson Current, Nashville, TN, 2005.

Bibby, A. "Invasion of the privacy snatchers," *Financial Times*, January 9, 2006.

Bose, I. and Pal, R. "Auto-ID: Managing Anything, Anywhere, Anytime in the Supply Chain," Communications of the ACM (48:8), 2005, pp. 100-106.

Cas, J. "Privacy in Pervasive Computing Environments – A Contradiction in Terms?," *IEEE Technology and Society Magazine* (24:1), 2004, pp. 24-33.

CGEY "RFID and Consumers: Understanding Their Mindset," Cap Gemini Ernst & Young, New York, NY, 2004.

Chappell, G., Durdan, D., Gilbert, G., Ginsburg, L., Smith, J., Tobolski, J. "Auto-ID on Delivery: The Value of Auto-ID Technology in the Retail Supply Chain," Auto-ID Center, MIT, Cambridge, MA, 2002.

Culnan, M.J. and Armstrong, P.K. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), 1999, pp. 104-116.

Culnan, M.J. and Bies, R.J. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2), 2003, pp. 323-342.

Davis, F. "Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology," *MIS Quarterly* (13:3), 1989, pp. 319-339.

De Jager, P. "Experimenting on Humans Using Alien Technology," in: Garfinkel, S. and Rosenberg, B. (eds.) "RFID", Addison-Wesley, Upper Saddle River, NJ, 2005, pp. 439-449.

Duce, H. "Public Policy: Understanding Public Opinion," Executive Briefing, Auto-ID Center, MIT, Cambridge, MA, 2003.

Eckfeldt, B. "What Does RFID Do for the Consumer?," *Communications of the ACM* (48:9), 2005, pp. 77-79.

Engberg, S., Harning, M. and Jensen, C. "Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience," Conference on Privacy, Security and Trust (PST 2004), Fredericton, 2004.

EPCglobal "Class 1 Generation 2 UHF Air Interface Protocol Standard Version 1.0.9," EPCglobal Inc., Lawrenceville, NJ, 2005.

EU "The RFID Revolution: Your voice on the Challenges, Opportunities and Threats," European Commission, Brussels, 2006.

Feldhofer, M., Dominikus, S. and Wolkerstorfer, J. "Strong Authentication for RFID Systems using the AES Algorithm," Workshop of Cryptographic Hardware and Embedded Systems (CHES 2004), Boston, MA, 2004.

Feldhofer, M., Wolkerstorfer, J. and Rijmen, V. "AES Implementation on a Grain of Sand," *IEE Proceedings on Information Security* (152:1), 2005, pp. 13-20.

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

Floerkemeier, C., Schneider, R. and Langheinrich, M. "Scanning with a Purpose – Supporting the Fair Information Principles in RFID protocols," in: Lecture Notes in Computer Science, Vol. 3598, Springer-Verlag, Berlin, 2005, pp. 214-231.

Gartner "Retail Question & Answer: U.S., U.K. Consumers Will Accept RFID in Exchange for Benefits," Gartner Group International, Stamford, CT, 2003.

Gefen, D., Karahanna, E. and Straub, D.W. "Trust and TAM in Online Shopping: An Integrated Model," *MIS Quarterly* (27:1), 2003, pp. 51-90.

Glidden, R., Bockorick, C., Cooper, S., Diorio, C., Dressler, D., Gutnik, V., Hagen, C, Hara, D., Hass, T., Humes, T., Hyde, J., Oliver, R., Onen, O., Pesavento, A., Sundstrom, K. and Thomas, M. "Design of ultra-low-cost UHF RFID tags for supply chain applications," *IEEE Communications Magazine* (42:8), 2004, pp. 140-151.

GS1 "La RFID appliquée à la logistique," Laboratoire RFID EPCglobal France, GS1 France, Issy-les-Moulineaux, 2005.

Günther, O. and Spiekermann, S. "RFID and the Perception of Control: The Consumer's View," *Communications of the ACM* (48:9), 2005, pp. 73–76.

Inoue, S. and Yasuura, H. "RFID Privacy Using User-controllable Uniqueness," RFID Privacy Workshop @ MIT, Cambridge, MA, 2004.

ITU "Ubiquitous Network Societies: The Case of Radio Frequency Identification," Document UNS/04, International Telecommunication Union, Geneva, 2005.

Juels A. and Pappu, R. "Squealing Euros:Privacy-Protection in RFID-Enabled Banknotes," Financial Cryptography '03, Guadeloupe, 2003.

Juels, A. "Minimalist Cryptography for RFID Tags," 4th International Conference on Security in Communication Networks (SCN 2004), Amalfi, 2004.

Juels, A. "RFID Privacy: A Technical Primer for the Non-Technical Reader," in: Strandburg, K. and Raicu, D.S. (eds.) "Privacy and Technologies of Identity: A Cross-Disciplinary Conversation," Springer, New York, NY, 2005, pp. 57-73.

Juels, A. "RFID Security and Privacy: A Research Survey," *IEEE Journal on Selected Areas in Communications* (24:2), 2006, pp. 381-394.

Juels, A. and Brainard, J. "Soft Blocking: Flexible Blocker Tags on the Cheap," Proceedings of the 2004 ACM workshop on Privacy in the electronic society, ACM Press, New York, NY, 2004, pp. 1-7.

Juels, A., Rivest, R. and Szydlo, M. "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," in: Proceedings of the ACM Conference on Computer and Communications Security, ACM Press, New York, NY, 2003, pp 103-111.

Karjoth, G. and Moskowitz, P. "Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced," Research Report RC23710, IBM Research Division, Zurich / Yorktown Heights, NY, 2005.

Kärkäinnen, M. "Increasing efficiency in the supply chain for short shelf life goods using RFID," *International Journal of Retail & Distribution Management* (31:10), 2003, pp. 529-536.

Karthaus, U. and Fischer, M. "Fully Integrated Passive UHF RFID Transponder IC With 16.7-µW Minimum RF Input Power," *IEEE Journal of solid-state circuits* (38:10), 2003, pp. 1602-1608.

Knights, D., Nobel, F., Vurdubakis, T. and Willmott, H. "Chasing shadows: control, virtuality and the production of trust," *Organization Studies* (22:2), 2001, pp. 311-336.

Kumar, R. "Interaction of RFID Technology and Public Policy," RFID Privacy Workshop @ MIT, Cambridge, MA, 2003.

Langheinrich, M. "Personal Privacy in Ubiquitous Computing – Tools and System Support," Ph.D. thesis No. 16100, ETH Zurich, Zurich, 2005.

Lessig, L. "Code and Other Laws of Cyberspace," Basic Books, New York, NY, 1999.

Loebbecke, C., Palmer, J. "RFID Becomes Fashionable in the Supply Chain: The Case of Kaufhof and Gerry Weber," Americas Conference on Information Systems (AMCIS), Acapulco, 2006.

McKnight, D.H. and Chervany, N.L. "What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology," *International Journal of Electronic Commerce and Business Media* (6:2), 2002, pp. 35-59.

McKnight, D.H., Cummings, L.L. and Chervany, N.L. "Initial trust formation in new organizational relationships," *Academy of Management Review* (23:3), 1998, pp. 472-490.

Odlyzko, A. "Privacy, economics, and price discrimination on the Internet," in: Proceedings of the 5th International Conference on Electronic Commerce (ICEC 2003), ACM Press, New York, NY, 2003, pp. 355–366.

Pavlou, P.A. "Integrating Trust in Electronic Commerce with the Technology Acceptance Model: Model Development and Validation," 7th Americas Conference in Information Systems, Boston, MA, 2001.

Perrin, S. "RFID and Global Privacy Policy," in: Garfinkel, S. and Rosenberg, B. (eds.) "RFID," Addison-Wesley, Upper Saddle River, NJ, 2005, pp. 15-36.

Ratnasingham, P. and Pavlou, P.A. "Technology trust: the next value creator in B2B electronic commerce," IRMA International Conference, Seattle, WA, 2002.

Rieback, M.R., Crispo, B. and Tanenbaum, A.S. "Is Your Cat Infected with a Computer Virus?," 4th IEEE Intl. Conf. on Pervasive Computing and Communications, Pisa, 2006.

Rivest, R. "Chaffing and Winnowing: Confidentiality without Encryption," *CryptoBytes* (4:1), 1998, pp. 12-17.

Sarma, S. "Towards the 5¢ Tag. Working Report," Auto-ID Center, MIT, Cambridge, MA, 2001.

Sarma, S. "A History of the EPC," in: Garfinkel, S. and Rosenberg, B. (eds.) "RFID," Addison-Wesley, Upper Saddle River, NJ, 2005, pp. 37-55.

Sarma, S., Weis, S. and Engels, D. "RFID Systems, Security & Privacy Implications," Workshop on Cryptographic Hardware and Embedded Systems 2002 (CHES 2002), Redwood City, CA, 2002

Shapiro, S. "The social control of impersonal trust," *American Journal of Sociology* (93:3), 1987, pp. 623-658.

Spiekermann, S. and Berthold O. "Maintaining privacy in RFID enabled environments – Proposal for a disable-model," Workshop on Security and Privacy in Pervasive Computing, Vienna, 2004.

Spinello, R.A. "Privacy Rights in the Information Economy," *Business Ethics Quarterly* (8:4), 1998, pp. 723-742.

Stajano, F. "RFID Is X-Ray Vision," *Communications of the ACM* (48:9), 2005, pp. 31-33.

Tellkamp, C., Angerer, A., Fleisch, E. and Corsten, D. "From Pallet to Shelf: Improving Data Quality in Retail Supply Chains using RFID," *Cutter IT Journal* (17:9), 2004, pp. 19-24.

Want, R. "The Magic of RFID," *ACM Queue* (2:7), 2004, pp. 41-48.

Weinberg, J. "RFID, Privacy, and Regulation," in: Garfinkel, S. and Rosenberg, B. (eds.) "RFID," Addison-Wesley, Upper Saddle River, NJ, 2005, pp. 83-97.

Weis, S., Sarma, S., Rivest, R. and Engels D. "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," 1st International Conference on Security in Pervasive Computing, Boppard, 2003.