

Faculty of Informatics

Faculty of Informatics - Papers

University of Wollongong

Year 2008

The RFID Value Proposition

B. D. Renegar*

K. Michael†

*University of Wollongong, mail@bentranet.com

†University of Wollongong, katina@uow.edu.au

This conference paper was originally published as Renegar, BD, & Michael, K, The RFID Value Proposition, COLLECTeR Iberoamérica, 25-27 June 2008, Madrid, Spain, 2008.

This paper is posted at Research Online.

<http://ro.uow.edu.au/infopapers/589>

The RFID Value Proposition

Benjamin D. Renegar¹ and Katina Michael²

¹ University of Wollongong, School of Information Systems and Technology, mail@bentranet.com
² katina@uow.edu.au

Abstract

Radio Frequency Identification (RFID) has the potential to revolutionize the retail industry, yet the linking of this automatic identification (auto-ID) technology to consumer goods has resulted in widespread concern over the potential privacy threats, primarily due to the aspect of traceability it could impose on consumers. As a consequence, privacy has come to be perceived as a barrier stopping RFID adoption in retail in its tracks. When investigating other complex information and communication technologies (ICT), it becomes apparent that consumers often sacrifice privacy in order to take advantage of some form of value afforded by the technology. This interplay between *value* and *privacy* is seen as a balance which must be favorable to the consumer to encourage acceptance. This study is focused on exploring this balance, with the addition of *control* as another important factor. The paper presents a review of literature, commencing with RFID technology itself and subsequently the value proposition that RFID offers retailers and consumers. It will investigate the privacy debate, looking at commonly expressed privacy concerns and the meaning of privacy. This will provide a basis for discussion of potential solutions that have been proposed.

Key words: RFID, privacy, value proposition, control

1 Introduction

Over the past decade, organizations have aggressively pursued the use of Radio Frequency Identification (RFID) as a means to better track, identify and control stock throughout the supply chain [1]. The linking of RFID, an automatic identification and data collection technology, to consumer goods, has resulted in widespread concern surrounding privacy issues [2], [3]. The mainstream media have been quick to expose these privacy concerns with most articles focusing purely on the technology's potential to track consumers without their knowledge or consent [4]. This has resulted in many major retail organizations around the world halting their RFID initiatives due to consumer backlash and many more organizations hesitant to proceed further [5], [6]. Privacy has grown to become a major issue blocking RFID's potential revolution in the retail industry [7]. This paper investigates the relationship between consumer value, privacy and control as it applies to the use of RFID in the retail industry. The research is set within the context of innovation studies, and it is hoped that the outcome will pave a way forward not only for RFID's adoption in retail, but for future advances in other automatic identification (auto-ID) technologies for which privacy is a major issue in adoption success.

2 RFID Technology

2.1 RFID Overview

Radio Frequency Identification has been in use in varying forms since World War II. It did not, however, become more practical until the 1960s. Since then, the technology has evolved and it now offers greater functionality, accuracy, read ranges and data transfer speeds [8]. It is more useful to view RFID as a system, one which consists of two important components: the tag and the reader [9]. Furthermore, there are two distinctly differently types of tags in use: active tags which are self-powered, and passive tags which have no power source of their own [10]. It is passive tags that hold most relevance for use in tagging consumer products as their elimination of a built-in power source enables them to be integrated into products in a cheaper, simpler and smaller fashion. In such a passive-tag system, the reader itself actually provides the power that enables the tags to respond by transmitting data. Therefore the tags by themselves are of no value unless coupled with a reader.

The technology is continually evolving, and as is further stressed by Want, RFID tags will too be a beneficiary of Moore's Law with improved read ranges, storage capacities and processing capabilities as time goes on. Another important point discussed by Lockett [10] is that RFID, like all technologies, involves a trade-off between a number of different variables. The price of the tags, their size, their performance and their storage capabilities must be balanced to the requirements of the application. Therefore, if the desire is to have a tiny, high performance tag, this will come at increased tag price. Finding the right balance to enable mass application in retail supply chains continues to be an important challenge [8]. Bound by the technical and economic restraints of the technology, RFID application in the retail supply chain is largely limited to tracking entire pallets or containers as opposed to individual items [11]. Nonetheless, as Weis [11] points out, the industry itself has widely publicized its intention to tag individual items in the future, a move that is being further facilitated by the development of the Electronic Product Code.

2.2 Electronic Product Code (EPC)

The fundamental idea behind the electronic product code (EPC) and its major goal is the development of an "Internet of things" which could enable a global system for tracking goods using a single numbering system for just about any kind of physical object [12]. Much work on the development of EPC standards began at MIT's Auto-ID Center, which in 2003 transferred the technology to EPCGlobal Inc. EPC has been developed to enable unique identification on the item level. This is achieved as each object carries its own code that distinguishes it from other objects of the same type, a contrast to the current dominant retail Uniform Product Code (UPC) standard which only identifies objects of a particular type [13]. One particular requirement in the development of the electronic product code standard was the requirement to enable it to sufficiently accommodate past, current and future needs in object identification. An important point emphasized by Theisse and Michahelles [12] is that EPC was not designed to replace existing numbering schemes, but to integrate and accommodate them in one overarching numbering system. Another important element of the EPC standard is the Object Name Space (ONS) which maps an EPC to an Internet IP address for storing additional information [9]. Sarma et al. highlight the importance of the ONS in addressing memory versus functionality problems associated with low-cost RFID tags, by allowing object information to be stored separately from the tag based on the unique identifier.

3 The RFID Value Proposition

3.1 For Retailers

The value proposition for retailers regarding RFID adoption is clearly expressed, both by vendors and in the literature. Both proponents and opponents of the technology agree that there is certain benefit in using the technology. Bansal

[14] expresses the primary benefit of RFID for retailers as “real-time supply chain visibility.” This is further highlighted by Kelly and Erickson [15], who explain how the ability to track products throughout the entire supply chain will deliver substantial competitive advantage. Supply chain “visibility” is essentially the ability to know where inventory is at any time by monitoring its progress from manufacturers to suppliers to retailers and then to the final consumer [10].

The ability of the technology to provide automatic identification of product data without human intervention or physical contact is central to RFID’s value proposition [14]. Kelly and Erickson [15] explain that, despite the technology being in its infancy, many prominent corporations, most notably Wal-Mart, have already begun planning and adopting RFID, demonstrating an already strong commitment to the technology. Successful implementation of many Efficient Consumer Response (ECR) initiatives, advocating the use of IT to maximize both consumer value and supply chain efficiency, has further been a contributor to surging RFID interest. Roussos [1] points in particular to RFID’s potential to improve vendor-managed inventory (VMI) efficiency by automating stock scanning, thus enabling continuous, accurate data flows to facilitate enterprise resource planning. Furthermore, the possibility of expanding the supply chain to the point of consumption (the consumer’s home) could facilitate an improved replenishment process.

Their key benefits of the technology for retailers as discussed by Kelly and Erickson [15] are summarized in table 1.

Business Process	Benefits
Inventory Control	Enable precise, real-time inventory counts, reduce out-of-stock situations, manage expiration dates, and reduce product dissipation (theft).
Manufacturing	Facilitate supply of raw materials, provide visibility of manufacturing process, and improve tracking of production processes.
Service	Improve checkout procedures with increased speed and accuracy, provide better customer service and improve customer satisfaction. Improved returns and warranty procedures limit fraudulent activities and provide greater customer convenience.
Transportation and Logistics	Limit disputes between manufacturers, suppliers and retailers by tracking delivery quantities at each step of the logistics process. Allow supply chain shrinkage to be readily identifiable, particularly with high value or sensitive goods.
Recalls	Provide a fast and efficient means to recall products by pinpointing the location of recalled goods.

Table 1 - Key retailer benefits [15]

These key benefits are added to further by Roussos [1], who includes improved user profiling, which supports more effective mass customization and marketing efforts. The ability to better understand consumer behavior and consumption patterns would provide retailers with further avenues to create a significant competitive advantage. The importance of this is evidenced by Roussos [1] in describing how ERP vendors have already begun implementing item-level recording in their products to support the improved supply chain processes which RFID enables.

3.2 For Consumers

Eckfeldt [5] makes an important assertion in discussing RFID’s value to consumers: “...the difference between successful and shunned RFID applications turns on delivery of clear, tangible value to the average consumer.” On these grounds, it is crucial that the value proposition of RFID as it applies to consumers be clearly expressed in order to promote adoption. Furthermore, Eckfeldt stresses that in assessing consumer benefit, organizations must consider consumers’ interests above their own else produce a solution that fails to provide a positive balance between risk and reward in the eyes of the consumer. In providing value to consumers, Eckfeldt suggests a three-way approach; providing peace of mind through involving security mechanisms, providing consumer convenience, and providing improved service. He further highlights that pivotal to all these solutions is a tangible consumer benefit.

The value proposition for consumers is highly dependent on the particular applications or usage of the technology. Extending the benefits to retailers, as described earlier, McGinity [7] stresses the key value to consumers, as better prices and product selection brought on by better efficiency at the back end, including reduced waste, shrinkage, and improved supply chain processes. However, as the systems have not been widely implemented, assessing or promoting such benefits would appear to be speculative at best as there is no basis to such claims. This is particularly apparent in many other proposed benefits of RFID which are based on applications of the technology that have not been deployed or tested in real-world environments, or are unrealistic given current technological capabilities.

EPCGlobal, the organization behind the EPC standard which is seen as the next generation of product identification, specifically describe a number of benefits for consumers [16]:

-
- Protecting consumers from counterfeit products
 - Tracking perishable food items to trace disease outbreak
 - Monitoring product freshness for goods with expiration dates
 - Providing more efficient means to recall defective products
 - Increasing product availability on shelves
 - Improving the recycling process
 - Generating economic growth

Whilst these benefits are similarly promoted by specific manufacturers and vendors, the number of notable failures of RFID already, highlights lack of understanding of RFID's value proposition by consumers, and poor communication of the value proposition by the manufacturers/retailers. This can further be highlighted in the Cap Gemini Ernst & Young study of 2003 which explored consumer perceptions of RFID [17]. The results indicated a severe deficiency in consumer awareness of the technology, with over 75% of respondents indicating that they did not recognize the utilization of RFID or what it had to offer.

Clothing retailers Benetton, Prada and Gap generated much hysteria when they began using RFID tags during trials in some of their stores in 2003. Further trials by Gillette, in co-operation with Wal-Mart also resulted in much outrage over the motive and purpose of the tags which were placed on individual razors. In all cases, the trials were cancelled due to consumer outcry, despite the potential benefits in using the tags to provide better services to customers. Importantly, though, in all cases, consumers were not made aware of the benefits. They were not told why the tags were on the products or what they were being used for. McGinity [7] critically comments that it is the retailer's responsibility to make the consumer see the tags as "advantageous rather than intrusive." She further comments again on the necessity for retailers to make consumers desire RFID in their lives.

In assessing the present RFID value proposition for consumers as it has been communicated in mainstream media, it is apparent that it has been defined insufficiently, unclearly or not at all. This certainly presents a contrast to RFID's value to business which, as described earlier, is quite clearly expressed and acknowledged. Individual studies, discussed later in this review, highlight that when demonstrated the value proposition of the technology and what it offers, consumers were positive and excited about the possibilities [18], [19]. Nevertheless, there is a clear need for this to be communicated more widely by RFID vendors, retailers and manufacturers.

4 The Privacy Debate

4.1 Privacy Concerns

The privacy debate centers on the tracking possibilities inherent in RFID technology. The argument is that, if the tags were to remain active after the consumer has left the store, the technology could provide retailers and manufacturers the ability to track an individual's movement and behavior in a clandestine manner [20]. This is introduced again by Roussos [1] who explains the technology's ability to "silently" retrieve and record unique identifiers as an important contributing factor towards consumer uneasiness. Garfinkel et al. [4] explain the problem voiced by activists such as Katherine Albrecht (director Consumers Against Supermarket Privacy Invasion and Numbering) as one of RFID "paving the way for a totalitarian state" wherein organizations can freely track the movement and behavior of individuals. Ironically, it seems that RFID manufacturers themselves provide ammunition to privacy activists, such as CASPIAN, by promoting RFID's ability to "tag anything and everything" whilst at the same time not adequately disclosing to the public RFID's capabilities or usage [11].

Garfinkel et al. [4] discuss seven key privacy threats that arise from RFID's capabilities: (1) action threat, (2) association threat, (3) location threat, (4) preference threat, (5) constellation threat, (6) transaction threat and (7) breadcrumb threat, which are summarized in table 2. These threats are also described by Hyangjin and Jeeyeon [3] in discussing the unique privacy concerns associated with RFID technology. Importantly, these threats are made possible largely due to the technology's ability to be read covertly, without requiring line-of-sight. The unique identification capabilities of RFID tags further contribute to the development of these threats. Such threats have given rise to much concern by privacy advocates. Eckfeldt [5] explains that many major companies, around the world, have already scrapped RFID plans following consumer backlash. If it weren't for the "haunting cries of privacy running afoot," many more companies would have tested and launched RFID initiatives [7]. The RFID failures of the likes of Gillette and Benetton as discussed earlier have highlighted the very real nature of the privacy issue and the impact it is having on RFID's adoption. This can also be seen clearly in the results of Cap Gemini Ernst & Young's consumer perception study of RFID. Their study highlighted privacy concerns as "the most significant issue among consumers in all countries" [17]. Consumer apprehension was greatest toward data being used by third parties, becoming the target of more direct marketing or being tracked via product purchases.

Threat	Definition
Action Threat	Inferring consumer behaviour based on tag actions.
Association Threat	Associating a consumer's identity with a tag's unique serial number.
Location Threat	Placing covert readers at specific locations to monitor tags.
Preference Threat	Determining user preferences based on tag data such as manufacturer, product type and value.
Constellation Threat	Even without associated consumer identity, a group of tags creates a "constellation" around the user to enable tracking.
Transaction Threat	Inferring transactions between individuals based on monitoring the "constellation" of tags.
Breadcrumb Threat	Building a trail of identity by collecting tagged items – a consequence of association.

Table 2 - Privacy threats [4]

4.2 Ubiquitous Computing and Privacy

Ubiquitous computing (UC) in general implies "tiny, wirelessly interconnected computers that are embedded almost invisibly into just about any kind of everyday object" [21]. The design, application and usage of RFID, and in particular the EPCGlobal standard, strongly position RFID as a core technology in the UC space. Research into the meaning of privacy explicitly in relation to RFID is lacking. However, much has been written on privacy in the context of ubiquitous computing, and as such, it is equally applicable to the present situation facing RFID.

The concept of privacy, what it means and how it is applied is a greatly complex, cross-disciplinary topic. It is important to understand the varying types of privacy. Langheinrich [22] describes five forms of privacy: media privacy, territorial privacy, communication privacy, bodily privacy, and information privacy. He points out, protection of the first four types of privacy has been well established through legal or constitutional rights. Protection of information privacy on the other hand, has presented a great problem as technologies have advanced and re-shaped its meaning continually of the past few decades. Boyle [23] in his attempt to create a "shared vocabulary" for privacy, emphasizes the complexity of defining privacy in his comment that "privacy is an overwhelmingly large and nebulous concept." In Boyle's lexicon of privacy, he deconstructs the ideas presented by Irwin Altman in his seminal work on privacy, and groups them based on three elements: (1) solitude (control over interpersonal relationships), (2) confidentiality (control of access to personal information) and (3) autonomy (control over what one does). Based on experience in ubiquitous computing, Boyle then further broadens the scope of these three elements such that solitude includes control over attention, confidentiality to include control over fidelity of information access, and autonomy by incorporating control over identity.

The theme of control is frequently discussed in the privacy literature, with many studies proposing that control and privacy are very closely connected, perhaps even synonymous with one another. Spiekermann [] in particular pinpoints that "privacy cannot be seen as separate from control; instead it is deeply intertwined with it." This concept of control is tackled by Spiekermann's assertion that user perceptions of privacy are really more about their perceptions of control.

4.3 Balancing Interests

Balancing the economic interests of business against the privacy interests of consumers is another cornerstone in the privacy debate. In reviewing the literature surrounding the value proposition for retailers and consumers above, it is apparent that business has, indeed, more to benefit from the implementation of the technology. Culnan and Bies [24] introduce three perspectives on consumer privacy: (1) the corporate perspective, (2) the activist perspective and (3) the centrist perspective. The corporate perspective sees corporations as the driving force for economic and societal development and thus they should have free access to consumers' personal information. The activist perspective on the other hand sees a major violation of the right to privacy and severe social costs if free-market forces are left unchecked, and personal information is available to anyone, for any purpose. In between such approaches, Culnan and Bies [24] introduce the centrist perspective, whereby corporate access to information should be balanced against the legitimate right consumers have towards protection of their privacy.

In addressing this balance, Culnan and Bies introduce the notion of the "second exchange," whereby consumers make a non-monetary exchange of their personal information in return for improved service, personalization and benefits. Importantly, they highlight that, for both organizations and consumers to realize the benefits, consumers must be willing to disclose their personal information and thus surrender some degree of their privacy. It is proposed, therefore, that people may be willing to accept a loss of privacy as long as there is an acceptable level of risk

accompanying the benefits. This idea of balance is touched on by many authors. Eckfeldt [5], for example, emphasizes the idea of risk again in stating that successful RFID applications over-compensate for any privacy fears. He furthers the idea of risk in proposing that consumers will accept the risks, if the application is worth the benefits. Langeheinrich's [22] discussion on privacy claims that privacy practices and goals must be balanced with the convenience or inconvenience associated with them. In balancing the interests of consumers against organizations, the important issue that seems to dominate, is the balancing of convenience and other terms of value for the consumer against the privacy incursion that is inevitable in providing such applications. The question that is raised but is yet to be critically analyzed is how much of our personal information must be sacrificed for the sake of convenience.

5 Proposed Privacy Solutions

5.1 Technical

In response to the privacy concerns that have been voiced, the industry has responded with varying approaches and schemes for protecting consumer privacy, many of which incorporate direct consumer control. The incorporation of consumer control in such solutions would appear appropriate given the linkage between control and privacy as discussed earlier. The key technological approaches as introduced by Bansal [14] include the "Kill Tag" approach, the "Faraday Cage" approach, and active or passive jamming. In a "Kill Tag" approach, the tag would be permanently disabled during checkout, preventing the tag from responding to or transmitting any data from that point on. Hyangjin and Jeeyeon [3] further mention that the EPC standard in particular, provides capability for exercising a "kill" command to deactivate the tag permanently. The "Faraday Cage" involves shielding tags and thus preventing them from being read, by placing them or wrapping them in metal foil. In the active jamming approach, consumers would carry their own device that would interfere with other RF signals and thus block successful tag reading. The passive jamming approach also involves the use of another device, but one which responds to read requests with random codes, thus confusing the reader. One of the major deficiencies of the above approaches is highlighted by Garfinkel et al. [4]. Activated tags do have post-sale value to consumers such as facilitating returns, repairs and warranty validation. Killing or deactivating tags on purchase consequently limits post-sale benefits the technology offers, and would prevent consumers from taking advantage of future-emerging services [6]. Garfinkel et al. [4] also introduce a number of other practical post-sale uses for RFID tags especially in regard to applications for the physically and mentally impaired. Thus, the disabling or crippling of tag functionality effectively destroys much of the innovative applications possible with the technology.

In search for a privacy solution that would not hinder the tag's potential use, researchers have proposed other solutions that do not intrinsically hinder tag functionality. Haifei, Hung, Jia and Ahn [25] propose an enterprise-wide privacy policy that manages and enforces, individual privacy preferences. This extends the work of the Privacy Preferences Project (P3P) working group of the World Wide Web Consortium (W3C). Their proposal sees two types of privacy policies, one which provides authorization over users; that is, who can access tag information, and authorization over data; what data can be stored and accessed from the tag. A similar scheme for protecting privacy, again based on the P3P project, is presented by Inseop, Byunggil, and Howon [26]. Their proposal incorporates access control mechanisms, authorization procedures, and user-established privacy preferences to enable appropriate information sharing. However, they conclude critically, that it would be "quite complicated and difficult to implement [the] proposed mechanism in real RFID-enabled environments." As they explain, the requirements for defining user privacy preferences, establishing policies, and developing secure communications links, complicates RFID's application in a retail environment. Hyangjin and Jeeyeon [3] introduce the idea of tag pseudonyms as another potential solution, whereby a number of identification numbers are rotated for each query, thus limiting tracking capabilities unless the reader knows all pseudonyms associated with that tag.

Encryption is also a widely discussed solution. However, as pointed out by Hyangjin and Jeeyeon [3] and again by Juels [20], the issues of key management, as well as the physical limitations of low-cost tags, pose a problem to this solution in practice. Furthermore, Ranasinghe, Engels and Cole [27], in developing their encryption solution for the technology, highlight in particular the cost constraints and "severe on-label resource constraints" for low-cost RFID systems (as would be implemented in retail environments) which provide a great challenge to the development of a hard-to-crack security mechanism.

Inoue and Yasuura [28], in viewing RFID usage throughout the entire lifecycle of an object from manufacture to disposal, suggest a two-level identification approach that would control the relationships between object and consumer. Their approach sees tags as having a public, static identification number that is combined with a private, user-assignable identification that can be applied to the tag when required. The question raised by this, and other similar solutions requiring user involvement, is their usefulness in a consumer/retail environment. Demanding such a level of user involvement, it seems, would detract from the usefulness of the technology and the benefits the technology provides in regard to convenience-oriented applications (see table 3).

Approach		Req'd Circuit	Proposed Schemes	Cost
Kill/Disable		N/A	Hardware processing Software processing	Low ↓ High
Keep-Alive Approach	Normal-tag approach	N/A	Electric wave interception Jammer wave Blocker tag	
	Smart-tag approach	Writable ROM	Anonymous-ID External re-encryption	
		Basic logic circuit	XOR-based OTP	
		Hash function/Common-key encryption	Hash-lock scheme Randomised hash-lock Hash-chain scheme	
		Public-key encryption	Internal re-encryption scheme	

Table 3 - Summary of technical approaches [6]

5.2 Regulatory and Legislative

From a legislation standpoint, the “RFID Right to Know Act of 2003” proposed by CASPIAN (Consumers Against Supermarket Privacy Invasion And Numbering) in the U.S., is one of the first legal attempts aiming to protect consumer privacy in regard to RFID deployment [3]. Furthermore, as discussed by Hyangjin and Jeeyeon, the EPCGlobal organization have themselves, established a set of regulatory guidelines for use on EPC-tagged products. Their guidelines emphasise the principles of consumer notification, education, and awareness of an RFID-tagged item. Kelly and Erickson [15] explain that the U.S. has taken a self-regulatory approach with privacy, whereby consumers are given few legal rights with respect to their personal information. Furthermore, companies in the U.S. are not required to offer consumers any choice over the collection of their information. The European Union, on the other hand, through the development of the “European Community Directive on Data Protection, 1998”, has decreed that information collection can only occur if the consumer has given consent, the information is necessary for the transaction, the information is required by law, or for law enforcement purposes. It is apparent that legislative attempts to protect privacy vary greatly by country, and furthermore, specific legislation dealing explicitly with RFID is very much non-existent or piecemeal at best. Whilst the industry points to self-regulation as a possibility, Kelly and Erickson [15] conclude that the benefits of the technology to retailers, and the inherent competitive advantage that results, will in reality, affect ethical retailer decisions regarding the collection of detailed consumer information.

The issue of regulation and legislation for protecting privacy becomes relevant when viewing privacy according to its “contextual integrity” [29]. Landwehr’s viewpoint that information collection is only a problem when individuals discover that an organization has used or shared their information inappropriately, beyond the relevant context, provides ground for appropriate regulations such to limit this happening. This raises another unanswered question of whether appropriate regulation would increase consumer acceptance of RFID, if consumers were guaranteed that the contextual integrity of their information were to be maintained.

5.3 Principles and Guidelines

Langheinrich [22] uniquely proposes that the ability to achieve a good balance between privacy and control can be facilitated by the development of a long-lasting relationship based on mutual trust and respect. In order to achieve such a relationship, Langheinrich points to the fair information practices enacted through the European Directive from which he extracts six important concepts for principles for privacy protection. These principles are summarized in table 4. As an outcome of the RFID privacy workshop held by the IEEE, and reviewed by Weis [11], privacy advocates and RFID manufacturers came to the consensus that full disclosure to consumers of tag presence and information collection is essential to RFID’s implementation. Furthermore, in providing “choice and consent,” consumers should be provided the right to kill, disable or remove and tags present on the items they purchase [11]. These guidelines and the principles outlined above, have also been published by the EPCGlobal organization, in their Guidelines on EPC for Consumer Products [30]. The technical, regulatory and legislative approaches to privacy protection discussed earlier in this section, align well to the privacy principles outlined in table 1.4. Whilst the development of a set of guidelines or principles such as that outlined provides a good framework for protecting privacy, the literature is still unclear as to whether such a framework would encourage acceptance of technologies such as RFID, in practice.

Principle	Implementation
Notice	Provide notification, announcement or declaration of information collection and perhaps more specifically the types of data collected through privacy policies available to consumers.
Choice and Consent	Receive explicit consent from consumers before collecting information and provide the option to opt-in or out. This could be implemented using digital signatures and authentication methods.
Anonymity and Pseudonymity	Perhaps in addition to, or instead of obtaining consent, enable consumers to remain anonymous by choice. This could be implemented by blocking/disabling/killing tags or removing unique identifiers.
Proximity and Locality	Maintain the boundaries of information collection relative to the place where it is required. This could be implemented by ensuring tags only respond to requests in the location the item is purchased or where the item's identification is relevant.
Adequate Security	Ensure information is protected from exploitation by other third parties. Security measures incorporating encryption and cryptography could maintain privacy of stored information.
Access and Recourse	Ensure that information collected is used only for stated purposes, and provide recourse for inappropriate use. Legislation can protect consumer rights against unlawful use of their personal information.

Table 4 - Privacy principles (based on [22])

5.4 RFID Limitations

The limitations of the RFID technology itself are often reported as a means of intrinsically reducing any privacy threat that could occur by third-party tracking. The privacy threat does not just apply to the retailer that sells the item containing the tag. There is also concern that other third parties, even other retailers, may also use tag data to monitor individuals or determine consumer behavior. Whilst many of these privacy concerns that have been raised are legitimate, many claims have no legitimate basis because they are beyond the practical and theoretical limits of the technology [11]. Alfonsi [2] further expresses agreement with industry experts who claim that the technical limitations of the technology itself limit potential privacy invasion. This is also mentioned by Roussos [1], who states that costs for both the tags, and the readers, is still too prohibitive for tagging all but high-value products. Alfonsi [2] further stresses the point that the typical read range of less than one meter is insufficient to trigger any real privacy threat.

In addition to the technical limitations present with the technology, economic factors also present a limitation that reduces the privacy threat. Alfonsi [2] again explains the reality that the price per tag is still too high for the technology to be widely distributed on a per-item basis. It is the possibility of item-level tracking that fuels most current debate in the privacy arena. Juels [20] critically explains that when dealing with passive RFID tags, it is not enough to speak about the read range of a tag, but rather the read *ranges*. He identifies four read ranges that influence the privacy threat. The nominal read range, is the typical reliable operating range of the tag under normal intended usage. The rogue scanning range is the read range of a tag when used with a high-powered reader. It is essentially the maximum read range of the tag. Tag-to-reader eavesdropping range, is the range at which another reader could monitor tag emissions without directly powering the tag itself. Finally, the reader-to-tag eavesdropping range is the range at which another reader could intercept transmission from a transmitting reader. The implications of these read ranges, varies, such that the nominal read range of usually a meter, limits the ability for privacy to be compromised by an unknown third party. The reader-to-tag eavesdropping range, on the other hand, enables information to be intercepted kilometers away [20].

6 Privacy Control in Practice

Eckfeldt [5] establishes the idea that despite any technical legitimacy to the many proposed solutions for privacy protection, the consumer perception of risk remains. He stresses that "Kill Tags" and other risk-reduction technologies and strategies cannot make up for a perceived level of risk if there is no value delivered by the RFID system. Roussos [1] summarizes an important point regarding privacy control mechanisms in stating that: "[privacy protection schemes] are unlikely to conclusively address consumer concerns because users interact with RFID systems at a much higher conceptual level." Roussos and Moussouri [19] conducted an early study aiming to investigate consumer perceptions of retail services provided by a ubiquitous, RFID-enabled supermarket.

The findings of their study revealed that many aspects of the RFID system were attractive for consumers, and most participants in the study did offset some degree of loss of privacy against the perceived value the system offered. The value proposition attracted “substantial interest” from the consumers, despite privacy concerns. However, even though consumers understood and appreciated the value of the system, the study found that certain aspects of the system were negatively received, particularly the invasiveness of the “home scenario” in which RFID would be used to monitor consumption patterns and provide additional services at the consumer’s home. Roussos and Moussouri conclude from their study that without providing consumers a degree of control over the system, they will not be persuaded to use it. They further point to the development of a trusting relationship between the consumer and the retailer as another key factor for acceptance.

Extending Roussos and Moussouri’s earlier study, Günther and Spiekermann [18] conducted another similar study on consumer perception of RFID with the crucial addition of privacy control mechanisms. The study provided two groups of 129 German citizens with a privacy-enhancing technology (PET) in an RFID-enabled retail environment. One group was able to exercise control over its privacy directly. For the other, control was delegated to an agent. The study showed that, “regardless of the PET employed, consumers [felt] helpless toward the RFID environment.” Günther and Spiekermann’s [18] study further highlighted that, even though their sample group was well informed of the benefits the technology provided, rating it both interesting and positive, they preferred the tags be killed instead of left activated. Additionally, the study found that better-educated consumers actually felt “even more helpless in the face of ubiquitous RFID technology.” This contradicts Roussos and Moussouri’s [19] earlier conclusion that providing control to the consumer would increase acceptance. The linkage between privacy and control that was discussed earlier, is also questioned by the results of this study. Spiekermann’s [21] own paper on measuring perceptions of control, emphasized that RFID environments that provide a positive feeling of control were likely to produce less of a concern regarding privacy invasion. Whilst it is possible that other privacy-enhancing solutions could induce such a positive feeling, it would seem that the real issue raised by Günther and Spiekermann’s study is that fear or perhaps other underlying motives, *combined* with user perceptions of privacy and control are the dominant factors in consumer acceptance of RFID. This is regardless of the value proposition, or privacy-controlling mechanisms (technical solutions, regulations, legislation, principles or guidelines) employed.

7 Conclusion

In assessing the value proposition of RFID for retailers and consumers, it is clear that whilst benefits for consumers have been well defined for a range of applications, they have not been communicated or expressed to consumers in an effective manner. One of the first opportunities that extend from the literature is thus to determine how this value proposition should be communicated to consumers such that they will desire RFID. Privacy concerns and threats are exacerbated by the covert and clandestine nature in which RFID can operate. Its ability to track consumers, monitor their behavior, purchase and consumption patterns, justifies consumer concerns about the technology. When viewing privacy in the context of control, it is suggested by the literature that perhaps the real concern is that users feel a lack of control over their private information as it would be collected and used in an RFID system. Nonetheless, it has been emphasized by a number of authors that consumers must accept such privacy loss if they are to take advantage of the benefits and conveniences RFID offers. This therefore presents another opportunity in the literature: what balance between privacy and convenience is required for consumers to accept and embrace the technology? This is linked also to the first opportunity in the sense that, if consumers do not understand the value proposition, how can they realistically perform such a “balancing equation” to make an informed decision? Privacy solutions have been presented from a number of angles: technical, legal and regulatory, and through guidelines and policies. Despite the range of solutions that have been proposed, the literature demonstrates that consumer perceptions of risk, trust, privacy and control, combined with fear, remain a barrier to acceptance, even in the presence of such control-enhancing solutions. This results in yet another opportunity in the literature: current studies have failed to provide understanding of consumer perceptions towards privacy and the underlying issues that affect such perceptions regardless of the privacy-controlling mechanisms or processes employed. The literature review also introduces the concept of auto-ID as a group of technologies of which RFID is a part. The literature highlights the topic of privacy as an important issue for auto-ID as a whole and importantly, presents the reality that many auto-ID technologies have already been adopted and accepted by society, despite the privacy concerns. Another opportunity is therefore exposed, in that, adoption characteristics and privacy concerns of various auto-ID technologies have not been linked together. The issue of convergence as it applies to auto-ID, highlights the importance of examining such relationships between the individual technologies as the technologies become increasingly intertwined.

References

- [1] G. Roussos, Enabling RFID in Retail, *Computer*, vol. 39, pp. 25-30, 2006.
- [2] B. J. Alfonsi, Privacy debate centers on Radio Frequency Identification, *IEEE Security & Privacy Magazine*, vol. 2, p. 12, 2004.
- [3] L. Hyangjin and K. Jeeyeon, Privacy threats and issues in mobile RFID, in 1st International Conference on Availability, Reliability and Security, Vienna, 2006, p. 5.

-
- [4] S. L. Garfinkel, A. Juels, and R. Pappu, RFID privacy: an overview of problems and proposed solutions, *IEEE Security & Privacy Magazine*, vol. 3, pp. 34-43, 2005.
- [5] B. Eckfeldt, What does RFID do for the consumer?, *Communications of the ACM*, vol. 48, pp. 77-79, 2005.
- [6] M. Ohkubo, K. Suzuki, and S. Kinoshita, *RFID Privacy Issues and Technical Challenges* vol. 48: ACM Press, 2005.
- [7] M. McGinity, RFID: Is This Game of Tag Fair Play?, *Communications of the ACM*, vol. 47, pp. 15-18, January 2004 2004.
- [8] R. Want, The magic of RFID, *Queue*, vol. 2, pp. 40-48, 2004.
- [9] S. Sarma, D. Brock, and D. Engels, Radio frequency identification and the electronic product code, *Micro IEEE*, vol. 21, pp. 50-54, 2001.
- [10] D. Luckett, The Supply Chain, *BT Technology Journal*, vol. 22, pp. 29-42, 2004.
- [11] S. A. Weis, RFID Privacy Workshop, *IEEE Security & Privacy Magazine*, vol. 2, pp. 48-50, 2004.
- [12] F. Theisse and F. Michahelles, An overview of EPC technology, *Sensor review*, vol. 26, pp. 101-106, 2006.
- [13] D. Brock, The electronic product code (EPC): a naming scheme for physical objects. MIT, Cambridge, MA: Auto-ID Center White Paper WH-002, 2001.
- [14] R. Bansal, Now you see it and now you don't [RFID Technology], *IEEE Microwave Magazine*, vol. 5, pp. 32-34, 2004.
- [15] E. P. Kelly and S. G. Erickson, RFID Tags: Commercial Applications v. Privacy Rights, *Industrial Management & Data Systems*, vol. 105, pp. 703-713, 2005.
- [16] EPCGlobal, *EPC Benefits for Consumers*, 2007.
- [17] C. Perakslis and R. Wolk, Social Acceptance of RFID as a Biometric Security Method, *IEEE Technology and Society Magazine*, pp. 34-42, Fall 2006 2006.
- [18] O. Günther and S. Spiekermann, RFID and the perception of control: the consumer's view, *Communications of the ACM*, vol. 48, pp. 73-76, 2005.
- [19] G. Roussos and T. Moussouri, Consumer Perceptions of Privacy, Security and Trust in Ubiquitous Commerce, *Personal and Ubiquitous Computing*, vol. 8, pp. 416-429, 2004.
- [20] A. Juels, RFID Security and Privacy: a Research Survey, *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 381-394, 2006.
- [21] S. Spiekermann, Perceived Control: Scales for Privacy in Ubiquitous Computing Environments, in 10th International Conference on User Modeling, Edinburgh, Scotland, 2005.
- [22] M. Langheinrich, Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems, in 3rd International Conference on Ubiquitous Computing, Atlanta, Georgia, 2001, p. 273.
- [23] M. Boyle, A shared vocabulary for privacy, in 5th International Conference on Ubiquitous Computing, Seattle, Washington, 2003.
- [24] M. J. Culnan and R. J. Bies, Consumer privacy: balancing economic and justice considerations, *Journal of Social Issues*, vol. 59, pp. 323-342, 2003.
- [25] L. Haifei, P. C. K. Hung, Z. Jia, and D. Ahn, Designing privacy policies for adopting RFID in the retail industry, in 2005 IEEE International Conference on Services Computing, Orlando, Florida, 2005, pp. 251-252.
- [26] K. Inseop, L. Byunggil, and K. Howon, Privacy Protection Based on User-defined Preferences in RFID System, in 8th International Conference Advanced Communication Technology, Korea, 2006, pp. 858-863.
- [27] D. C. Ranasinghe, D. W. Engels, and P. H. Cole, Security and Privacy Solutions for Low-cost RFID Systems, in 2004 Intelligent Sensors, Sensor Networks and Information Processing Conference, 2004, pp. 337-342.
- [28] S. Inoue and H. Yasuura, RFID privacy using user-controllable uniqueness, in RFID Privacy Workshop, Cambridge, MA, 2004.
- [29] C. E. Landwehr, Speaking of Privacy, *IEEE Security & Privacy Magazine*, vol. 4, pp. 4-5, 2006.
- [30] EPCGlobal, *Guidelines on EPC for Consumer Products*, 2005.