

*Faculty of Informatics*

*Faculty of Informatics - Papers*

---

*University of Wollongong*

*Year 2009*

---

The privacy-value-control harmonization  
for RFID adoption in retail

B. D. Renegar\*

K. Michael†

\*IBM

†University of Wollongong, [katina@uow.edu.au](mailto:katina@uow.edu.au)

This article was originally published as Renegard, BD & Michael, K, The privacy-value-control harmonization for RFID adoption in retail, IBM Journal of Research and Development, 53(2), 2009, 1-16. Original journal information available <[a href="http://www.research.ibm.com/journal/rd/" >here</a>](http://www.research.ibm.com/journal/rd/)

This paper is posted at Research Online.

<http://ro.uow.edu.au/infopapers/713>

Title: The privacy-value-control harmonization for RFID adoption in retail

Authors: B.D. Renegar, K. Michael

Abstract:

Over the past decade organizations have aggressively pursued the use of radio frequency identification (RFID) as a means to better identify, control and track stock throughout the supply chain. RFID has the potential to revolutionize the retail industry. However the application of this automatic identification (auto-ID) technology to consumer goods has resulted in widespread concern over potential privacy threats, primarily due to the aspect of subject-to-object traceability. As a consequence, privacy has come to be perceived as a barrier to RFID adoption in retail, as consumers seek to control data about themselves. When investigating other complex technologies, it becomes apparent that consumers often sacrifice perceived privacy and control to take advantage of some form of value afforded by the given technology (e.g. the mobile telephone). The interplay between privacy, value, and control must be harmonious to encourage future acceptance of RFID by consumers. Through the investigation of multiple case studies of auto-ID technologies and services this study aims to discover the factors influencing the development of the privacy-value-control (PVC) trichotomy. The case studies are supported by an online survey which aims to explore the role education and awareness play in influencing perceptions towards RFID's value proposition and its potential privacy threats.

## 1 Introduction

### 1.1 Overview

Over the past decade, organizations have aggressively pursued the use of radio frequency identification (RFID) as a means to better identify, control and track stock throughout the supply chain. The linking of RFID, an automatic identification and data collection technology, to consumer goods, has resulted in widespread concern surrounding privacy issues. 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. Prior to 2004, this resulted in many major retail organizations around the world temporarily halting their RFID initiatives due to consumer backlash and many more organizations hesitant to proceed further [1]. Since that time numerous U.S. and European-based large retailers have either adopted RFID or conducted trials [2]. While privacy may not be the single biggest issue stifling the deployment of RFID, it has acted to delay uptake in the retail industry [3]. This paper is about the relationship between consumer privacy (P), value (V) and control (C) as it applies to the use of RFID in the retail industry.

### 1.2 Aims and Objectives

The aim of this study is to explore whether an appropriate harmonization between consumer privacy, value and control can be established. The contribution of this study is in examining all three factors with respect to RFID. There are two vital considerations in achieving this aim: (1) how consumer awareness influences perceptions and consequently the development of such a balance, and (2) the balance evident in other similar auto-ID technologies and services which have already been adopted successfully. The aim of the study will be achieved through five objectives (Figure 1):

1. To identify RFID's value proposition for consumers.
2. To analyze the value, privacy and control paradigm in the context of already-adopted technologies and services.
3. To identify consumer perceptions of RFID, its value proposition, and privacy issues.
4. To assess how education and awareness affect perceptions of value, privacy and control.
5. To determine whether an appropriate harmonization between value, privacy and control can be achieved.

### 1.3 Radio-Frequency Identification

RFID is best characterized as an automatic identification technology that uses radio waves to identify objects. In the context of this study, the specific RFID technology of interest is passive tags, which are tiny transponders that can be embedded or attached to an object requiring identification. These transponders, as small as a grain of rice, do not have a power source of their own; rather, they use the energy from an incoming radio frequency signal to transmit stored data to the reader. The most important characteristic of RFID technology in relation to the tagging of consumer goods is that it is contactless as opposed to line-of-sight which is a requirement of bar codes. For Gen 2 EPC UHF (electronic product code/ultra high frequency) passive tags, the read range is typically 3.5 meters while the write range is 2 meters depending on the reader in question and the

environmental conditions. It is not uncommon today to achieve reads of up to 8 meters away using these tags. The ability for RFID tags to be read covertly is the central cause of concern amongst privacy advocates.

## 2 Previous Works

There are a number of studies that have been conducted which have aimed to understand aspects of consumer acceptance of RFID. The key outcomes are summarized in Table 1. Many other works have proposed solutions to protect and enhance privacy and afford consumers a level of control [4], [5], [6]. These solutions are typically technology-based, legislative or regulatory in nature. Despite the different privacy solutions, a number of studies critically highlight that consumer perceptions and fear of the technology brought about by a lack of understanding remain [7], [8]. It is apparent from such studies that the real issue becomes one of fear or other underlying motives, that, when combined with perceptions of privacy and control, motivate a consumer's acceptance of RFID technology.

Table 1 – Key quantitative study outcomes

Study	Outcome
[8], [9], [10]	Regardless of which privacy-enhancing technologies are used, fear remains.
[7]	Consumers understood the value proposition but were still concerned about privacy implications.
[11]	Cultural dimensions affect the way in which consumers view the privacy threat.
[12]	Consumers feel a lack of control over the technology and a great power distance.

### 2.1 Privacy

The classic definition of privacy is provided by Westin [13], as the “claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” This study is primarily focused on information privacy which is described by Clarke [14] as “the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves.” Of primary concern in regard to RFID usage in retail, is the collection of personal information that pertains to consumer shopping preferences, actions and behavior. It is the collection, use and disclosure of this information, particularly when it may be incorrect or unverified, to identify, track and monitor individuals without their awareness or express approval, that is commonly recognized as one of the most prominent threats. It is important to understand that Clarke's definition, along with other definitions of privacy from Altman [15], Schoeman [16], and Margulis [17], all emphasize that privacy is not separate from control, rather it is “deeply intertwined with it” [9].

### 2.2 Value

Value in this study will be viewed in terms of the benefits RFID technology affords consumers. It is how an individual prizes a certain outcome against all others [18]. The

value proposition to consumers for RFID usage in retail is generally phrased in terms of convenience. It is an equation of all the positive factors that interest the individual. It can include cost savings, time reductions, efficiency, personalization, safety and security, as well as convenience and other tangible and intangible benefits. Therefore, in creating a harmony between privacy, value and control, it is a harmonization between consumer willingness to lose some degree of privacy versus the strength of the retailer's value proposition for using the technology [19]. The value proposition can essentially be seen as a combination of benefits versus risks that consumers will evaluate in their decisions and perceptions.

### 2.3 Control

Inness [20] is clear that in characterizing the function of privacy in terms of control or restricted access there are ramifications for the normative value we accord privacy. For the purpose of this study, control becomes a relevant dimension of RFID acceptance, because it is only through a perceived level of control of their own personal information, that consumers will feel their privacy is being maintained [21]. It relates to the individual's ability to control the information that is collected and stored by the RFID technology or its ability to identify, record or track that individual's actions. The level of control that is provided either inherently through the technology or by the service provider, whether that be perceived or real, is seen as an important element that, when combined with the value proposition, can affect consumer acceptance.

### 2.4 The Privacy Debate

The privacy debate has developed due to the identification and tracking possibilities inherent in the 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 [22]. This is introduced by Roussos [23] who explains the technology's ability to "silently" retrieve and record unique identifiers as an important contributing factor towards consumer uneasiness. Garfinkel et al. [5] 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. Such threats have given rise to much concern by privacy advocates. In 2005, Eckfeldt [24] explained that many major companies, around the world, had already scrapped RFID plans following consumer backlash. If it were not for the "haunting cries of privacy running afoul," many more companies would have tested and launched RFID initiatives [1]. 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" [25].

### 2.5 The Value Proposition for Consumers

The value proposition for RFID's application in retail is an important topic that underscores consumer acceptance of RFID. What is apparent in surveying the literature is that whilst the benefits for RFID have been clearly defined and expressed for retailers, they have not been so clearly communicated to consumers. Eckfeldt [24] 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.” Furthermore he 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. He further highlights that pivotal to all these solutions is a tangible consumer benefit. McGinity [1] 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.

## 2.6 Balancing Interests

Balancing the economic interests of business against the privacy interests of consumers is another cornerstone in the privacy debate. Culnan and Bies [19] 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 the notion of “second exchange,” is introduced whereby consumers make a non-monetary exchange of their personal information in return for improved service, personalization and benefits [19]. 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 balancing interests is touched on by many authors. Eckfeldt [24], 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 [26] 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. It must be underscored that an underlying assumption made in this study by the authors is that privacy incursions, especially in the form of breaches in information privacy, are inevitable in the adoption of any emerging mass-market technology, and even more so if that technology happens to be wireless or mobile.

## 3 Methodology

### 3.1 Research Strategy and Design

This study used a combination of qualitative and quantitative approaches; a qualitative case study of auto-ID-related technologies and services, and a quantitative analysis of an online survey. The multiple case studies included, the mobile phone, electronic toll collection (ETC), e-Passports and loyalty programs. The online survey was used to analyze individual consumer perspectives towards RFID’s value proposition and privacy threats relative to education and awareness. The conceptual framework for the case study approach taken is illustrated in figure 2.

### 3.2 Data Collection

#### 3.2.1 Case Studies

Data collection for the case studies used multiple sources of evidence, including documents such as books, media reports, journal articles, papers, whitepapers, corporate information and marketing materials. The documents were sourced from libraries (offline), databases, online journals, media organizations and corporate, government and institutional websites. The data collection was an iterative process, starting with a broad search strategy involving the key topics under investigation, with more targeted searches conducted thereafter (Table 2).

Table 2 Document Collection- Types, Sources and Search Terms

Data Types	Data Sources	Search terms
<ul style="list-style-type: none"> <li>• Books</li> <li>• Magazines</li> <li>• Reports</li> <li>• Articles</li> <li>• Papers</li> <li>• Theses</li> <li>• Dissertations</li> <li>• Product descriptions</li> <li>• Whitepapers</li> <li>• Marketing materials</li> </ul>	<ul style="list-style-type: none"> <li>• Libraries</li> <li>• Databases               <ul style="list-style-type: none"> <li>• ACM</li> <li>• IEEEExplore</li> <li>• ProQuest</li> <li>• ScienceDirect</li> <li>• Emerald</li> <li>• Factiva</li> <li>• Springerlink</li> </ul> </li> <li>• Online journals               <ul style="list-style-type: none"> <li>• Communications of the ACM</li> <li>• IEE Review</li> <li>• IEEE Security and Privacy magazine</li> <li>• IEEE Technology and Society magazine</li> <li>• Journal of Consumer Marketing</li> <li>• MIS Quarterly</li> </ul> </li> <li>• Media organizations               <ul style="list-style-type: none"> <li>• CNET</li> <li>• BBC</li> <li>• New York Times</li> <li>• Wired</li> </ul> </li> <li>• Web sites               <ul style="list-style-type: none"> <li>• Government</li> <li>• Corporate</li> <li>• Personal</li> <li>• Groups</li> <li>• Institutions</li> </ul> </li> <li>• Company/product web sites</li> </ul>	<ul style="list-style-type: none"> <li>• Core terms               <ul style="list-style-type: none"> <li>• Mobile phones</li> <li>• Cell phones</li> <li>• Mobile communications</li> <li>• Electronic toll payment</li> <li>• Electronic toll collection</li> <li>• Automated toll payment</li> <li>• Intelligent transportation systems</li> <li>• E-Passports</li> <li>• Biometric passports</li> <li>• RFID passports</li> <li>• Loyalty programs</li> <li>• Loyalty cards</li> <li>• Rewards programs</li> <li>• Loyalty schemes</li> </ul> </li> <li>• Additional terms               <ul style="list-style-type: none"> <li>• Privacy</li> <li>• Value</li> <li>• Benefits</li> <li>• Convenience</li> <li>• Control</li> <li>• Statistics</li> <li>• Usage</li> <li>• Penetration</li> <li>• Acceptance</li> <li>• Consumer</li> </ul> </li> <li>• Case-study-specific examples, organizations, topics, events, etc.</li> </ul>

#### 3.2.2 Online Survey

Data collection for the online survey was administered at [www.rfidsurvey.org](http://www.rfidsurvey.org) for a period of 75 days, from July 10, 2007 through September 23, 2007. The online survey was openly accessible to all Internet users; however, specific recruitment occurred in the

form of electronic and physical mail-outs. The online survey collected data based on 28 questions structured into four separate sections. The first section collected general demographic information as well as information about the participants' awareness and education. The second section questioned participant perceptions of RFID's value proposition, asking participants to rank both awareness and importance against a list of proposed RFID benefits. The third section focused on assessing value and privacy in regard to a number of other technologies such as mobile phones, smart cards, loyalty programs, e-Passports, GPS car navigation and electronic toll collection. Four of these technologies are featured in the case study analyses. The final section of the survey questioned perceptions of RFID's potential privacy threats; again presenting participants with a list of threats and having them rank awareness and concern of such threats. It must be emphasized that there were also several opportunities for respondents to reply to open comments throughout the survey.

### 3.3 Data Analysis

#### 3.3.1 Narrative Discussion and Content Analysis

Qualitative "content analysis" was used to discover regularities between the four technologies/ services under investigation. By structuring the case studies in the same manner, around the themes of privacy, value and control, a comparison between each case study was made. The analysis focused on the significance of the technology given its penetration and usage rates, despite the presence of privacy threats, and is presented in a narrative discussion format. The text-mining tool Leximancer was used to analyze the documents collected, and the open commentary provided by survey respondents. Leximancer assisted in uncovering the main concepts contained within the text and showed how these were inter-related [27].

#### 3.3.2 Statistical Analysis

The purpose of the statistical survey analysis was to identify causal relationships by conducting multivariate analyses on the survey participants' perceptions of RFID's potential threats and its potential value given a number of typical usage scenarios. Perceptions of threat and value were also analyzed with regard to a number of other auto-ID technologies. Using the SAS JMP software package, a common "score" for RFID's value and threat, as well as the other auto-ID technologies' value and threat, was arrived at by aggregating the rankings given by participants to relevant questions. The participant's awareness of RFID and its potential usage was also found in this way using linear regression analysis.

## 4. Case Studies

This section will present case studies that explore the adoption and acceptance of a number of technologies and services within the context of privacy, value and control [28].

### 4.1 Mobile Phone

The value proposition of the mobile phone extends from the convenience offered by its inherent mobility. In a study conducted by Häkkinen and Chatfield [29] regarding perceptions of mobile phone privacy, it was shown that over 82% of respondents considered their mobile phone a "private device." The mobile phone presents a number of

unique privacy threats, yet interestingly, as indicated by the aforementioned statistic, such privacy threats are seldom discussed or thought of by end users [30]. Richtel [31] explains how many citizens in the U.S., for example, are completely unaware that government authorities can track their movements by monitoring the signals that are emitted from the handset. The mobile phone also presents other privacy concerns in regard to the interception of signals by unauthorized persons [32]. Theoretically, users can exercise control over other parties tracking their location by simply turning off their phone. However, in doing so, they prevent access to the phone's features which provide the value in the first place.

#### 4.2 Electronic Toll Collection

The key value proposition that electronic toll collection systems offer is convenience and time saving. Such a system eliminates the burden to have cash available to make toll payments and provides individuals and corporations the convenience of an account which can provide better tracking of toll expenditure with more convenient payment options [33].

Caldwell [34] highlights two potential privacy concerns with regard to electronic toll collection. The first is illegitimate use of drivers' personal information regarding their payment information, movement and driving habits that could be accessed if electronic records are compromised through a "cyber-break-in." This was demonstrated when a programmer was successfully able to view account details and usage information for users of one of the largest ETC systems in the United States [35]. The second potential concern is legitimate use of such information by government authorities or road operators who can use the information to monitor driving patterns and behavior of thousands of motorists. This could extend to include other potential uses such as traffic surveillance in regard to monitoring driver speeding and stolen vehicles [36]. Court cases in the U.S. have already demonstrated the potential for toll-tracking information to be used to verify an individual's whereabouts and movements. The states of Delaware, Illinois, Indiana, Maryland, Massachusetts, New York and Virginia have all released E-ZPass toll records in response to court orders for civil matters such as divorce. The states of Maine, New Hampshire, New Jersey and Pennsylvania only release electronic toll records for criminal cases [37].

#### 4.3 e-Passports

The greatest value of the e-Passport as stressed by most issuing authorities is the enhancement to security they are purported to provide through the digital storage of passport information [38]. Certainly, given the current level of importance placed on national security, governments have been keen to introduce this technology as a means of providing more stringent monitoring of individuals entering and exiting the country.

The privacy concerns surrounding e-Passports are primarily related to the ability to access passport information without contact, a capability afforded by the use of RFID to store the passport's data contents. Juels, Molnar and Wagner [39] identify six key areas of concern outlined in Table 3. Globally, it is reported that over 50 million e-Passports have been issued, which again emphasizes that despite the privacy concerns, the technology has undoubtedly been deployed "successfully" [40]. Some States have shielded the contactless microchip in a metal jacket to prevent the chip from being read

when the passport is closed [41]. If not provided, a sheet of aluminum foil will equally prevent unauthorized access of personal data on the e-Passport [42].

Table 3 – Privacy threats and the e-Passport (adapted from [39])

Threats	Description
Clandestine scanning	RFID communication between the reader and passport does not require authentication or encryption under ICAO (International Civil Aviation Authority) guidelines.
Clandestine tracking	The use of chip ID on protocol initiation would identify individual passports if it is unique and allow tracking even if the chip data cannot be read.
Skimming and cloning	Digital signatures do not prevent passports being cloned, as they cannot tie the data to a particular passport or chip.
Eavesdropping	At locations where passports may be opened frequently, the potential for eavesdropping on communication between the passport and reader would be problematic.
Cryptographic weaknesses	Once a reader knows the key, there is no mechanism for revoking access, thus giving the reader the ability to scan the passport in perpetuity.

The media has also been quick to highlight potential failures with the technology, demonstrated by the exposure given to Lukas Grunwald who successfully cloned the U.S. e-Passport and then dumped the contents onto an ordinary contactless smart card [43]. A further threat was also exposed by Kevin Mahaffey and John Hering who demonstrated how an explosive device connected to an RFID reader could be triggered when a U.S. citizen carrying an e-Passport came within reach of the reader [43]. Given the mandatory nature of passports, there is very little individuals can do to avoid using one when traveling abroad. There is also little an individual can do to control how government authorities access and use the information on the passport when they are entering a foreign country.

#### 4.4 Loyalty Programs

In the case of loyalty programs, the value proposition is critical for encouraging consumer use and for developing the brand loyalty which the programs aim to achieve. A number of elements are described by Yi and Jeon [44] that determine such value in a loyalty program. They include: (1) the cash value of rewards, (2) the choice of rewards, (3) the aspirational value of rewards, (4) the likelihood of achieving the rewards, and (5) how easy the loyalty scheme is to use.

The major privacy threat that extends from the use of loyalty programs is the ability to tie purchases of specific products to individual consumers and monitor their purchasing behavior over time. A study conducted by Graeff and Harmon [45] found that in regard to loyalty programs, consumer perceptions were typically positive and most consumers did not associate such schemes with the collection and use of personal information. Loyalty programs are the ultimate demonstration of the trade-off consumers make of their privacy in order to gain something of value: a benefit, reward, convenience or saving [46].

A key element of consumer loyalty programs is their opt-in nature [47]. Consumers are also given control over their personal information by government regulations which in most countries give consumers the right to know exactly what information retailers are collecting and how it is being used.

#### 4.5 Discussion

It would appear given the widespread usage of the cases detailed, that privacy has not been a barrier to their adoption and consequent acceptance by society. Whilst the privacy concerns still exist and indeed, many individuals remain concerned about their privacy in relation to such technologies and services, on the whole it would seem that consumers have accepted each technology either because:

- The value proposition or level of control present, balances against the privacy issues (mobile phones, electronic toll collection, and loyalty programs), or
- Participation/usage is mandatory and the appropriate safeguards to privacy are in place (e-Passports).

Table 4 – Summary of privacy threats

	Mobile Phone	Electronic Toll Collection	e-Passports	Loyalty Programs
Action	Actions can be inferred by monitoring phone location.	Actions can be inferred by monitoring tag usage/toll payment.	Actions can be inferred through the monitoring of passport usage.	Actions can be inferred by monitoring usage of loyalty cards or redemption of rewards.
Association	Individuals are serialized through the international mobile equipment identity (IMEI) of their phone and phone number.	Individuals are serialized through their tag ID number/account number.	Individuals are serialized through their passport number.	Individuals are serialized through their membership number.
Location	Location can be established through triangulation or GPS.	Location can be established by tag usage.	Location can be established by passport reads.	Location can be established by loyalty card usage.
Preference	N/A	N/A	N/A	Consumer preferences can be determined by monitoring purchases and behavior.
Transaction	N/A	N/A	N/A	Transactions can be inferred through usage of a loyalty card.
Breadcrumb	A trail of actions can be inferred by phone location and usage.	A trail of actions is created through toll payments.	A global trail is created each time the passport is read.	A trail is created of individual purchases and overall shopping behaviors.

In the case of the mobile phone, the value has become so ubiquitous that it is no longer even discussed. This ubiquity in terms of value would explain the lack of concerns consumers have towards their privacy in regard to mobile phone usage. For electronic toll collection, individuals have embraced the convenience aspects and it would seem that the simplicity of the technology (simply install the tag and forget about it) has again resulted in a general lack of concern about privacy issues. Loyalty programs are also clearly

driven by their value proposition. Of the four case-studies discussed, the e-Passport is the only one where usage is almost completely mandatory for those wishing to travel internationally and also where individuals have very little control over how their e-Passport is used by authorities. A summary of the key elements of value, privacy and control for each of these technologies is provided in table 5.

Table 5 – Key elements of value, privacy and control

	Value	Privacy	Control
Mobile Phone	<ul style="list-style-type: none"> <li>- Convenience in communication</li> <li>- Convenient mobile applications and services</li> </ul>	<ul style="list-style-type: none"> <li>- Location tracking through triangulation or GPS</li> <li>- Interception of voice or data communication</li> </ul>	<ul style="list-style-type: none"> <li>- Users can turn off their phone – although inconvenient</li> </ul>
Electronic Toll Collection	<ul style="list-style-type: none"> <li>- Convenience in toll payment</li> <li>- Reduced congestion and traffic queuing</li> </ul>	<ul style="list-style-type: none"> <li>- Location tracking and monitoring through RFID tag</li> <li>- Database of toll payments and movements</li> </ul>	<ul style="list-style-type: none"> <li>- Individuals can pay cash tolls or use alternative routes – although sometimes not an option or inconvenient</li> </ul>
e-Passports	<ul style="list-style-type: none"> <li>- Improved security, individual and national</li> <li>- Convenient passport processing</li> <li>- Global identity authentication</li> </ul>	<ul style="list-style-type: none"> <li>- Skimming, cloning or eavesdropping of passport contents</li> <li>- Global databases including biometric information</li> <li>- Potential for function creep</li> </ul>	<ul style="list-style-type: none"> <li>- Individuals have no other option when traveling abroad.</li> <li>- Shield the passport when not in use</li> </ul>
Loyalty Programs	<ul style="list-style-type: none"> <li>- Retail savings</li> <li>- Rewards</li> <li>- Sense of self-importance and belonging</li> </ul>	<ul style="list-style-type: none"> <li>- Collection of personal information</li> <li>- Sharing of information between organizations</li> <li>- Monitoring of purchases and shopping behavior</li> <li>- Targeted marketing based on personal preferences</li> </ul>	<ul style="list-style-type: none"> <li>- Individuals can opt-out of participating or conduct business elsewhere</li> </ul>

#### 4.6 The Harmonization between Privacy, Value and Control

A key outcome that arises from the case studies presented is the varying relationship between three elements (privacy, value, control) and thus the balance each technology or service provides. It is clear, that in order to gain acceptance, privacy issues must be offset by value and control. This trichotomous relationship is illustrated in figure 3 which is based on the auto-ID technology responses covered in the survey.

In the case of mobile phones, it is evident that a somewhat low level of control is acceptable, given the relatively low vulnerability of individual privacy and the medium level of value the technology provides. With electronic toll collection, the vulnerability of user privacy is depicted to be in the medium range, yet as users can exercise some degree of control over their privacy by removing the tag or opting to use alternative routes or payment methods, control is depicted as being in the medium range. This medium range in regard to privacy and control is offset by a high level of value evident in the convenience the technology affords. With regard to e-Passports, the government provides very little control. Furthermore, the value offered to the individual is in real terms also very low. Finally, with loyalty programs, a high vulnerability of individual privacy which

arises from the vast amount of personal information collected is offset by a high level of control offered by providers by allowing consumers to freely opt-out of such programs. The privacy risk is also further offset by the high level of value which such schemes must offer to encourage consumers to participate.

In the case of mobile phones, electronic toll collection and loyalty programs, it is apparent that acceptance had to be earned through a favorable balance that was offered to consumers. In the case of e-Passports where the balance is unfavorable (as shown in figure 3), acceptance was not generally required as the technology was made mandatory by government authorities and the ICAO.

## 5. Survey Analysis

The threats listed in the survey are potential threats of RFID (i.e. perceived) that have been drawn out from the literature as the major causes for consumer concern over RFID's usage in retail.

*Awareness* refers to the aggregated score of each survey participant's responses to a number of questions that dealt with perceptions of RFID and other auto-ID technologies. Specifically, the awareness score was calculated by the sum of responses in which participants ranked using a Likert scale of 1 to 5, knowledge on a list of 12 RFID related topics.

### 5.1 Sample Respondents

There were 142 survey responses. The majority (61.1%) of surveys were completed by Australians. The U.S. had the second largest number of responses (27.4%), with other responses recorded from countries such as Canada, Germany, Spain and the United Arab Emirates. Figure 4 demonstrates that age plays a determining factor in awareness of RFID. It is seen clearly in figure 4 how awareness generally decreases with age.

#### 5.1.1 The effect of awareness on RFID's perceived value

Figure 5 shows the relationship between awareness and RFID's value proposition which is statistically significant. It is seen that as awareness increases, the participants' rankings towards RFID's value proposition decreases. It then follows that the more highly aware participants are, that is, those who know more about the technology and all its corresponding issues, place less importance on the value the technology provides and instead balance that more appropriately against the issues the technology carries with it.

#### 5.1.2 The effect of awareness on RFID's perceived threat

Surprisingly, it would seem that awareness plays little role in an individual's ability to perceive the privacy threats that the technology could introduce if it were to be implemented. This suggests perhaps that participants, regardless of their awareness of RFID, are able to appreciate the privacy issues based on their previous life experiences, particularly with other technologies which may present similar issues.

#### 5.1.3 Influence of RFID's value proposition on perceived threat

The higher individuals rank the RFID value proposition, the lower they rank the privacy threat. This would suggest that individuals, who place importance on the value RFID offers, are slightly less concerned about the privacy threats. In this sense, elements

of the value proposition such as convenience, may win out over potential threats that an individual may face in terms of privacy.

#### 5.1.4 Perceived threat of RFID as compared to other auto-ID technologies

A key element of the survey was the ranking participants provided on both value and privacy concern in regard to a number of other related technologies in widespread use today. There was a statistically strong relationship found between the perceived privacy threat of these other technologies and RFID usage in retail. In essence, respondents who were concerned about their privacy in relation to the other technologies were just as likely to be concerned about their privacy if RFID were to be adopted in retail.

#### 5.2 Analysis of Open Comments

Analysis of the comments revealed a great range of attitudes, ranging from individuals who were strongly focused on potential privacy issues, to individuals who saw the technology as something quite positive and thus balanced this against the potential privacy issues. There were also many individuals who highlighted controls that would need to be in place to make the technology acceptable.

In regard to privacy, there were a number of respondents who made clear expressions of their privacy concern. Comments such as “I should have my right to privacy,” “...it invades on our personal freedoms,” “It’s too obtrusive,” and “...this technology is a violation of people’s right to privacy” clearly express strong feelings towards the potential for RFID to erode privacy of the individual. Many individuals also stressed that whilst they could see the value, or see the positives, they were not convinced that potential privacy issues would be managed effectively. This is well represented in the comment that “the benefits ascribed to RFID technology for the retail trade are commendable, but I have zero confidence that they will be achieved, and, instead, consumers will be subjected to more advertising, intrusion, and loss of privacy than ever.”

Contrarily, there were a number of respondents who clearly valued the technology despite any potential privacy issues. One individual commented that “...only someone trying to hide something or [run] from something would think this system is not a positive thing.” Another individual commented that “...the benefits for consumers ... far outweigh the privacy issues that are envisaged” and that “...the privacy issues would sort themselves out in time.” A couple of respondents also critically point out that indeed, this study assumes RFID technology will replace the bar code at some point. They highlight that the technologies are more complementary to each other, and that the value of placing RFID tags on every item is not justified by the present cost in doing so.

It would seem that the majority of users approach the technology with the idea that control would best balance the value against the privacy issues. The clear majority of comments expressed that the design of RFID systems should incorporate privacy protection from the outset. A common theme is seen in one user’s comment that “if proper privacy and security architectures were implemented AND ENFORCED, the deployment of RFID systems need not be so problematic...” And again from another respondent, “if privacy concerns were taken into account and proper privacy-enhancing technologies were implemented and used, we could have the benefits without the drawbacks...”

Regulation and legislation were also pointed out by a number of respondents as important means of providing individuals with control over their privacy. Some consumers noted they would be happy with using the technology provided if “the technology was adequately regulated...”

On the whole, it is apparent that most users are more concerned about the misuse of their information than the actual collection of it. Whilst privacy could be protected by a range of controls, the potential for the technology (as with any technology) to be misused and abused by “the low integrity sector of society” represents the greatest fear.

### 5.3 Overall Perceptions of RFID in Retail

Together with the open comments, survey participants were also asked to provide a general ranking of RFID technology as it would be used in retail. Surprisingly, given the comments made and also the fact that the mean ranking in regard to privacy threats and RFID was 77%, the majority of individuals were neutral to very positive towards the technology (figure 7). It would seem that most individuals can appreciate the technology and although the privacy issues exist, feel that they can be overcome, offset or controlled in some manner.

### 5.4 Discussion

A number of important outcomes are evident from the statistical analysis presented in this paper. These are summarized below:

- As awareness of RFID and its issues increase, the relative importance of RFID’s value proposition decreases
- Awareness of RFID and associated issues, does not affect perception of RFID’s threats
- The perceived privacy threat, and value of RFID in retail is relative to an individual’s existing feelings towards other technologies/services with similar issues to RFID

The most important observation in analyzing the results from the survey is the generally contradictory nature of respondents. It is not uncommon for participants to indicate RFID as privacy-threatening, yet at the same time still be a member of a loyalty program, or use a mobile phone.

## 6. Survey Results Comparison with Case Studies

In comparing the means of some of the technologies and services that were included in both the online survey and the case studies, it is evident that concern surrounding RFID’s potential privacy threat in retail is considerably greater than the concern participants express for the other technologies. It is the lower end of the spectrum, where users have little to no concern regarding privacy and technologies such as the mobile phone and electronic toll collection, and services like loyalty programs, where it is quite evident that concern about RFID privacy threats is higher than should be expected. The key outcome that this exposes is the lack of harmonization in the current privacy, value and control offering that RFID in retail presents.

In the case studies, it was highlighted that appropriate harmonization between value and control could offset privacy issues. This is reflected in the little concern participants in this survey placed on such technologies and services. Thus, the high rankings of RFID

privacy threats demonstrate more education would be required to convince consumers of the value and control they would have over RFID usage. It is, however, important to understand that these rankings were given for technologies/services that are already in widespread use, whereby individuals have had time to understand and experience them in the context of their own lives. The privacy threat rankings individuals gave RFID, in many cases evidence the lack of awareness towards RFID. If consumers were to actually experience RFID usage in retail and place it in context with their own activities, it could be seen that rankings of the privacy threats may be significantly different, and perhaps more in line with the other technologies/services highlighted.

Therefore, it could be concluded, based on all of the key results presented in this paper that creating a favorable harmony between privacy, value and control is perhaps an unrealistic notion when the technology has yet to be implemented. When there is such a divergent level of awareness amongst the greater population, striking a balance that is acceptable to all is an improbable task. It is therefore suggested that acceptance of RFID in retail may ultimately come over time, after adoption, as users become intimately experienced with its usage. Consequently, privacy, value and control will become perpetually adjusted based on the feedback and behaviors of society, and in that sense a favorable balance will eventually be developed in the same manner as shown by many of the case studies.

## 7. Principle Outcomes

The principle outcomes of the study can be summarized as follows:

1. RFID's value proposition has not been well communicated to consumers.
2. Privacy has not been a barrier to the adoption of many technologies/services with similar issues to RFID in retail.
3. The harmonization achieved between privacy, value, and control is largely dependent on the individual, the technology and the provider.
4. A favorable harmonization whereby privacy is offset by value and control encourages consumer acceptance.
5. Consumer awareness of RFID and its issues affect perceptions of value.
6. Awareness does not affect perceptions of privacy threats.
7. The perceived value, and privacy threats presented by RFID, is relative to an individual's pre-existing feelings towards other similar technologies.
8. Concerns surrounding RFID were disproportionately higher than other previously adopted technologies despite similar privacy issues.
9. A harmonization between privacy, value and control is unrealistic prior to adoption and can only be achieved once consumers can be educated through experience with the technology.

The case studies highlighted the importance of a harmonization between privacy, value and control in influencing consumer acceptance and adoption. The online survey demonstrated the effect awareness has on perceptions and the disproportionately high rankings given for RFID privacy concerns.

The most significant outcome that is arrived at from the combined analysis of the case studies and the online survey is that achieving a harmony between privacy, value, and control for RFID adoption in retail is unrealistic at this point in time. With such differing

levels of awareness and education, differing expectations and differing perceptions, achieving a harmony that is favorable to all consumers now would be an improbable task. It is also evident in reviewing the literature that there have already been significant attempts to address privacy issues and provide individuals with a degree of control, yet the privacy concern still remains. This furthers the notion that it is unlikely privacy concerns can be resolved prior to the technology's adoption and use by consumers.

RFID in retail can certainly achieve a favorable harmonization which offsets privacy risks with significant value and consumer control. It is more realistic, however, for this harmony to be achieved after adoption, when consumers can be educated through their experiences, and whereby society will consequently shape the balance as the technology's impact becomes more evident. This progression is depicted in figure 8.

## 8. Conclusion

In a society where it seems we are increasingly surrounded by technologies, governments, organizations and institutions monitoring every move we make and collecting vast amounts of personal information, privacy has grown to become an ardently debated topic. As a society and as individuals, our right to privacy is paramount, yet in the wake of technologies which afford us great value, there will always be some privacy sacrifice that must be made. This study has not sought to dismiss privacy, or promote it, but rather address it in the realistic context it plays in an environment of technological innovation that is driven by society itself. Ultimately, acceptance of a technology with privacy issues will always be a balancing act, a harmonization between privacy, value and control.

## 9. Cited references (and notes):

1. M. McGinity, "RFID: Is This Game of Tag Fair Play?," *Communications of the ACM* 47, 15-18 (2004).
2. A. Schurr, "RFID deployment ramps up," *Network World*, 26 August (2008).
3. K. Michael and L. McCathie, "The pros and cons of RFID in supply chain management," *International Conference on Mobile Business, Sydney* (2005) pp. 623-629.
4. R. Bansal, "Now you see it and now you don't [RFID Technology]," *IEEE Microwave Magazine* 5, 32-34 (2004).
5. S. L. Garfinkel, A. Juels, and R. Pappu, "RFID privacy: an overview of problems and proposed solutions," *IEEE Security & Privacy Magazine* 3, 34-43 (2005).
6. L. Hyangjin and K. Jeeyeon, "Privacy threats and issues in mobile RFID," *1st International Conference on Availability, Reliability and Security, Vienna*, (2006) pp. 510-514.
7. G. Roussos and T. Moussouri, "Consumer Perceptions of Privacy, Security and Trust in Ubiquitous Commerce," *Personal and Ubiquitous Computing* 8, 416-429 (2004).
8. O. Günther and S. Spiekermann, "RFID and the perception of control: the consumer's view," *Communications of the ACM* 48, 73-76 (2005).
9. S. Spiekermann, "Perceived Control: Scales for Privacy in Ubiquitous Computing Environments," *Conference on User Modeling, Edinburgh, Scotland*, (2005).
10. S. Spiekermann, *User Control in Ubiquitous Computing: Design Alternatives and User Acceptance*. Aachen, Shaker Verlag, (2008).
11. G. Ng-Kruelle, P. A. Swatman, J. F. Hampe, and D. S. Rebne, "Biometrics and e-Identity (e-Passport) in the European Union: End-user Perspectives on the Adoption of a

- Controversial Innovation," *Journal of Theoretical and Applied Electronic Commerce Research* 1, pp. 12-35 (2006).
12. G. Ng-Kruelle, P. A. Swatman, D. S. Rebne, and J. F. Hampe, "The Price of Convenience: Privacy and Mobile Commerce," *Quarterly Journal of Electronic Commerce* 3, 273-385 (2002).
  13. A. F. Westin, *Privacy and Freedom*. USA, The Bodley Head Ltd, (1970).
  14. R. Clarke, "What's 'Privacy'?", in Workshop at the Australian Law Reform Commission 2008 <http://www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html> (2006).
  15. I. Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Monterey, CA, Brooks/Cole, (1975).
  16. F. D. Schoeman, "Philosophical Dimensions of Privacy: An Anthology." Cambridge, Cambridge University Press, (1984).
  17. S. T. Margulis, *Contemporary Perspectives on Privacy*. London, Blackwell Publishing, (2003).
  18. B. D. Renegar and K. Michael, "The RFID Value Proposition," presented at Sixth Collector Iberoamerica - Collaborative Electronic Communications and eCommerce Technology Research, Madrid, Spain, (2008) pp. 1-10.
  19. M. J. Culnan and R. J. Bies, "Consumer privacy: balancing economic and justice considerations," *Journal of Social Issues* 59, 323-342 (2003).
  20. J. C. Inness, *Privacy, Intimacy and Isolation*. USA, Oxford University Press, (1996).
  21. J. R. Averill, "Personal control over aversive stimuli and its relationship to stress," *Psychological Bulletin* 80, 286-303 (1973).
  22. B. J. Alfonsi, "Privacy debate centers on Radio Frequency Identification," *IEEE Security & Privacy Magazine* 2, 12 (2004).
  23. G. Roussos, "Enabling RFID in Retail," *Computer* 39, 25-30 (2006).
  24. B. Eckfeldt, "What does RFID do for the consumer?," *Communications of the ACM* 48, 77-79 (2005).
  25. C. Perakslis and R. Wolk, "Social Acceptance of RFID as a Biometric Security Method," *IEEE Technology and Society Magazine*, 34-42 (2006).
  26. M. Langheinrich, "Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems," *Proceedings of the 3rd International Conference on Ubiquitous Computing*, Atlanta, Georgia, (2001), pp. 273-291.
  27. Leximancer, "Leximancer Concept Miner," <http://www.leximancer.com/resources/leximancer-concept-miner.pdf> (2008).
  28. B. D. Renegar, K. Michael, and M. G. Michael, "Privacy, Value and Control Issues in Four Mobile Business Applications," presented at The Seventh International Conference on Mobile Business, Barcelona, Spain, (2008), pp. 30-40.
  29. J. Häkkinen and C. Chatfield, "Toward social mobility: 'It's like if you opened someone else's letter': user perceived privacy and social practices with SMS communication," Salzburg, Austria, (2005).
  30. N. Swartz, "Mobile Phone Tracking Scrutinized," *Information Management Journal* 40, 16 (2006).
  31. M. Richtel, "Live tracking of mobile phones prompts court fights on privacy," in *The New York Times*, <http://www.nytimes.com/2005/12/10/technology/10phone.html?pagewanted=1&ei=5088&en=2011ce3dd6b43183&ex=1291870800&partner=rssnyt&emc=rss> (2005).

32. R. Whitaker, *The End of Privacy: How total surveillance is becoming a reality*. New York, The New Press, (1999).
33. SRI Consulting, "Electronic Toll Collection," in ITS Canada <http://www.infoworld.com/articles/hn/xml/00/10/25/001025hnezpass.html> (1996).
34. C. Caldwell, "A Pass on Privacy?," in *The New York Times* <http://www.nytimes.com/2005/07/17/magazine/17WWLN.html?ex=1279339200&en=c1f10d3de06adea6&ei=5088> (2005).
35. E. Grygo, "New Jersey Turnpike electronic toll collection system hacked," in *InfoWorld* <http://www.infoworld.com/articles/hn/xml/00/10/25/001025hnezpass.html> (2000).
36. D. Loukakos and M. Benko, "Electronic Toll Collection," in *ITS Decision* [http://www.calccit.org/itsdecision/serv\\_and\\_tech/Electronic\\_toll\\_collection/electronic\\_to ll\\_collection\\_summary.html](http://www.calccit.org/itsdecision/serv_and_tech/Electronic_toll_collection/electronic_to ll_collection_summary.html) (2007).
37. C. Newmarker, "Toll records catch unfaithful spouses," in *USA Today: Associated Press*, [http://www.usatoday.com/tech/news/surveillance/2007-08-10-ezpass\\_N.htm](http://www.usatoday.com/tech/news/surveillance/2007-08-10-ezpass_N.htm) 10 August (2007).
38. M. Meingast, J. King, and D. K. Mulligan, "Embedded RFID and everyday things: A case study of the security and privacy risks of the U.S. e-Passport," presented at *IEEE International Conference on RFID*, Texas, (2007), pp. 971-978.
39. A. Juels, D. Molnar, and D. Wagner, "Security and privacy issues in e-Passports," *IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks*, Athens, Greece, (2005).
40. Scarmig, "E-Passport: Doorway to the Panopticon" <http://www.strike-the-root.com/62/scarmig/scarmig1.html> (2006).
41. International Civil Aviation Organization, "Machine Readable Travel Documents (MRTDs): History, Interoperability, and Implementation," in *ISO/IEC JTC1 SC17 WG3/TF1 for ICAO-NTWG*, 23 March (2007).
42. M. Sirotich, "ePassport Security Under the Microscope," in *From Dataveillance to Uberveillance and the Realpolitik of the Transparent Society*, Vol. 2, K. Michael and M. G. Michael, Eds. Wollongong, University of Wollongong, (2007), pp. 257-280.
43. K. Zetter, "Hackers clone e-Passports," in *Wired* <http://www.wired.com/science/discoveries/news/2006/08/71521?currentPage=1> (2006).
44. Y. Yi and H. Jeon, "Effects of loyalty programs on value perception, program loyalty, and brand loyalty," *Academy of Marketing Science* 31, 229 (2003).
45. T. Graeff and S. Harmon, "Collecting and using personal data: consumers' awareness and concerns," *Journal of Consumer Marketing* 19, 302-318 (2002).
46. Anonymous, "Grocery store loyalty card use is strong despite privacy concerns," in *About.com: Coupons/Bargains*, [http://couponing.about.com/od/groceryzone/a/loyalty\\_cards.htm](http://couponing.about.com/od/groceryzone/a/loyalty_cards.htm) (2007).
47. M. Bosworth, "Loyalty cards: Reward or threat?" [http://www.consumeraffairs.com/news04/2005/loyalty\\_cards.html](http://www.consumeraffairs.com/news04/2005/loyalty_cards.html) (2005).

## Biographies:

Benjamin D. Renegar, IBM Global Business Services, IBM Centre, 601 Pacific Highway, St. Leonards, NSW, Australia 2065 (brenegar@au1.ibm.com). Ben Renegar is a recent graduate from the University of Wollongong, having completed a Bachelor of Information and Communication Technology degree at the end of 2007 with the award of 1<sup>st</sup> class honours. For this degree program he completed a thesis on RFID adoption in the retail industry with a focus on the balance between value, privacy and control. He was also awarded the PriceWaterhouseCoopers award for the highest grade in this program. Subsequently, Mr. Renegar has been employed by IBM as a Graduate Consultant in the Application Innovation Service Delivery organization.

Katina Michael, University of Wollongong, NSW, Australia 2500 (katina@uow.edu.au). Dr. Michael is a Senior Lecturer in the School of Information Systems and Technology in the Faculty of Informatics at the University of Wollongong. She received a Bachelor of Information Technology degree from the University of Technology, Sydney (UTS) in 1996 and a Ph.D. degree in information technology and communications from the University of Wollongong in 2003. Before joining the University of Wollongong in 2002 to teach and research in eBusiness, she worked as a senior network and business planner at Nortel Networks. In 2000 Katina received Nortel's top talent award for work completed on 3G mobile networks in Asia. Dr. Michael is a senior member of the Institute of Electrical and Electronics Engineers and a Board Member of the Australian Privacy Foundation.

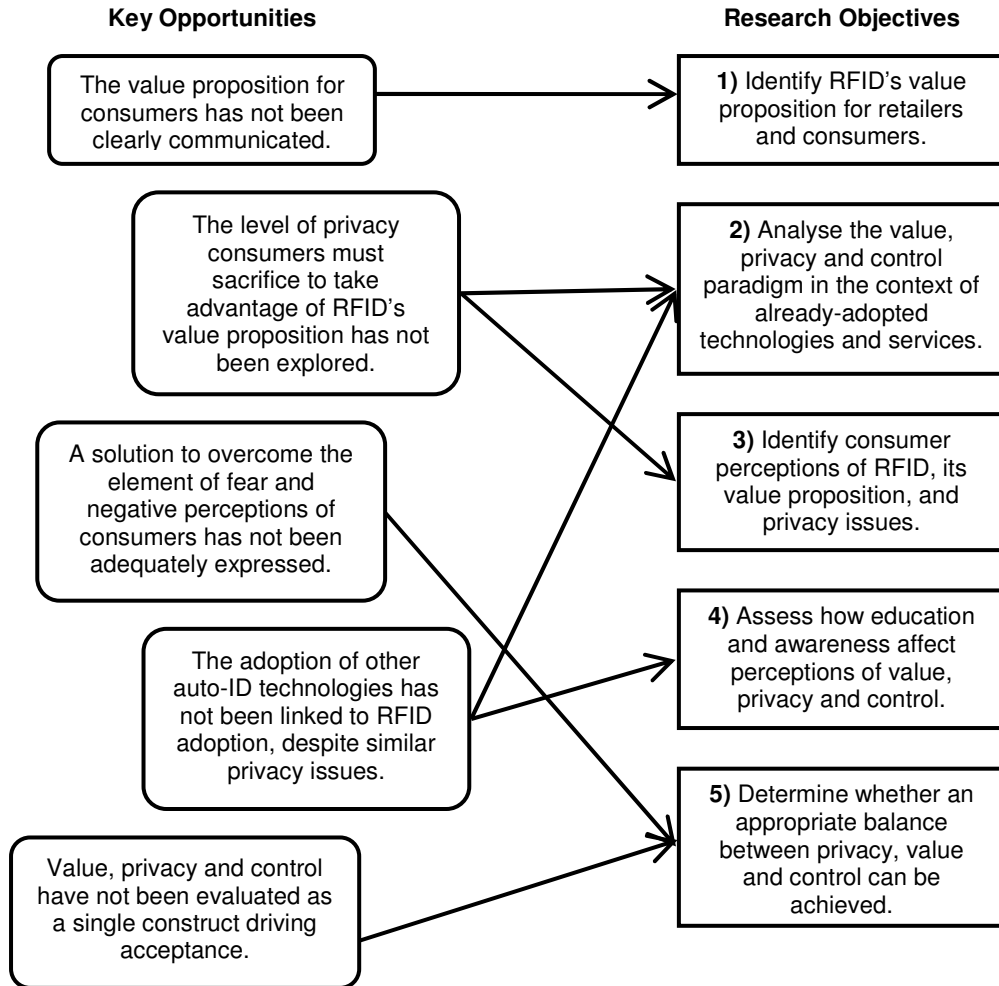


Figure 1 – Key opportunities and their relationship to research objectives

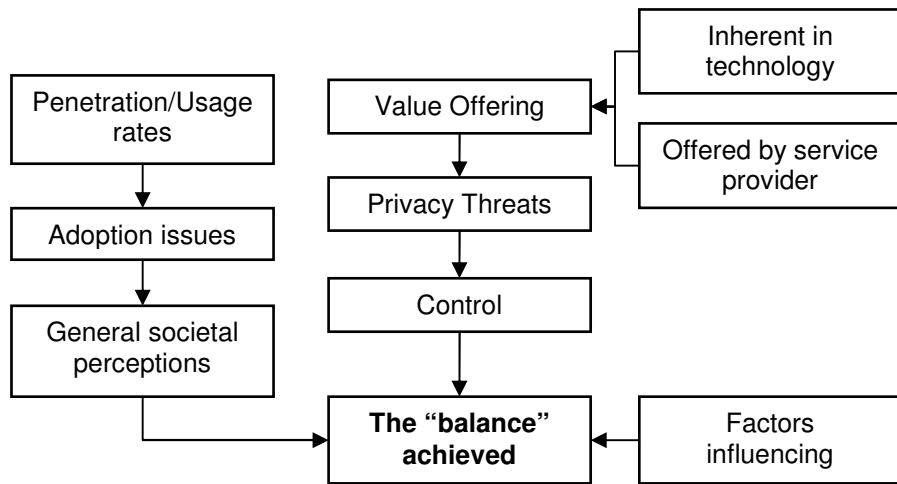
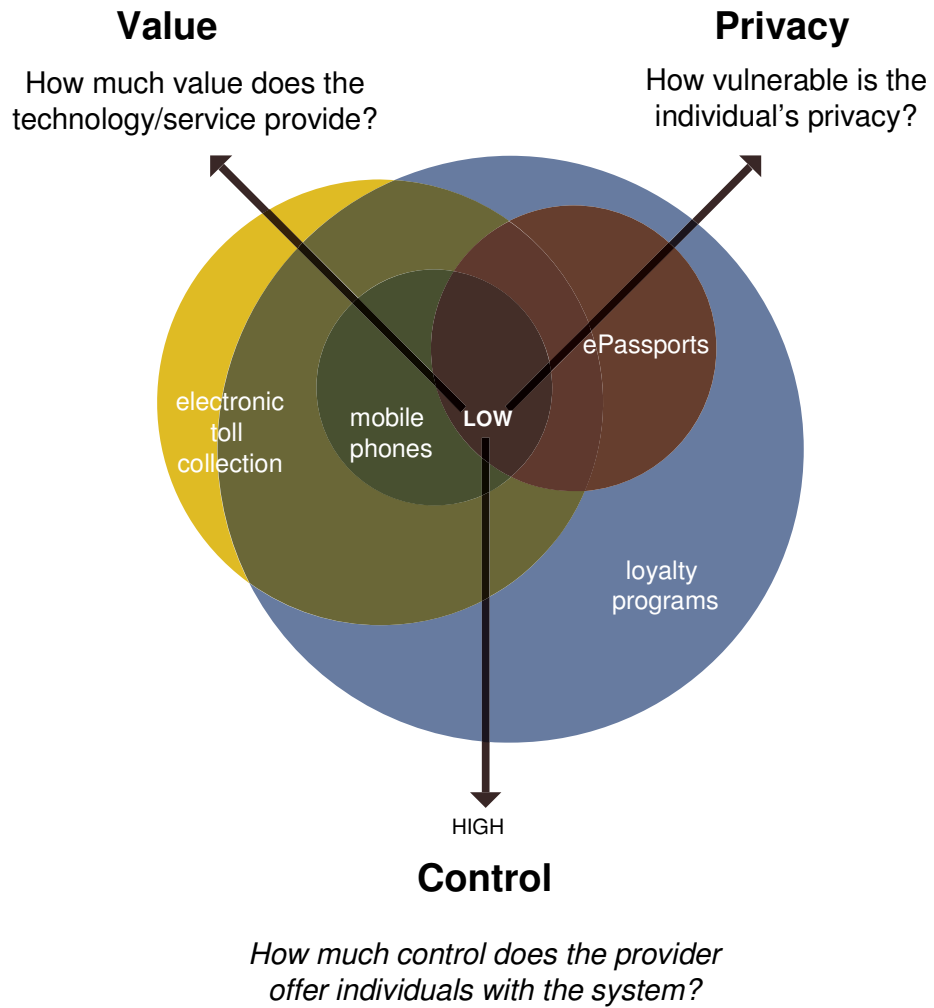


Figure 2 – Case study conceptual framework

Figure 3 – Balancing privacy, value and control



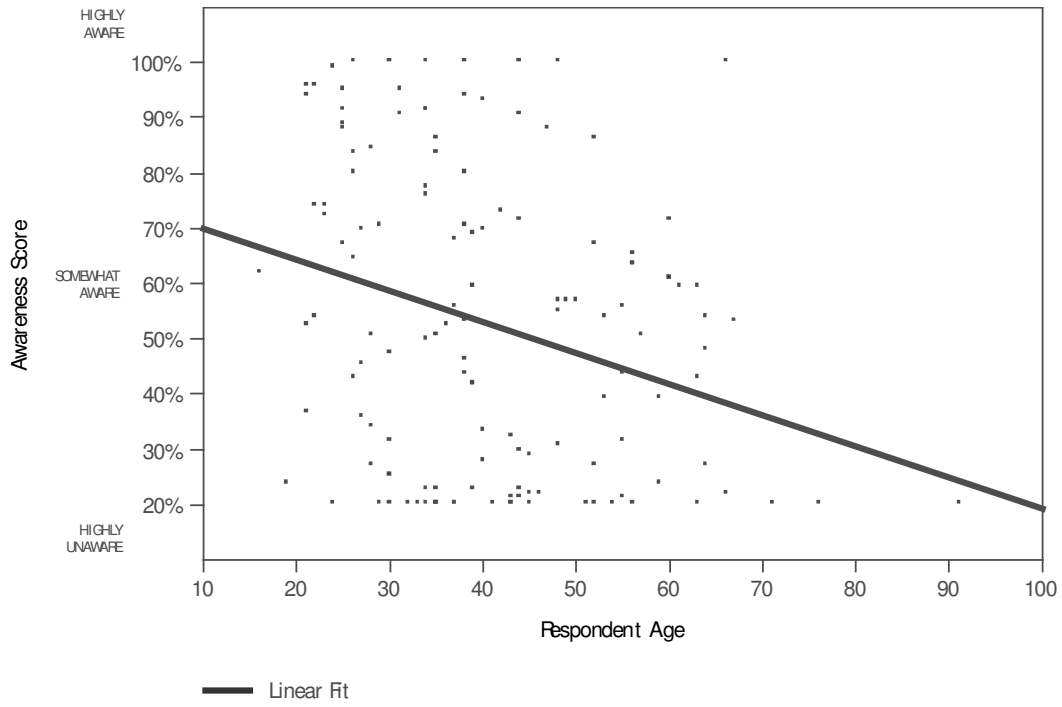


Figure 4 – The relationship between age and awareness

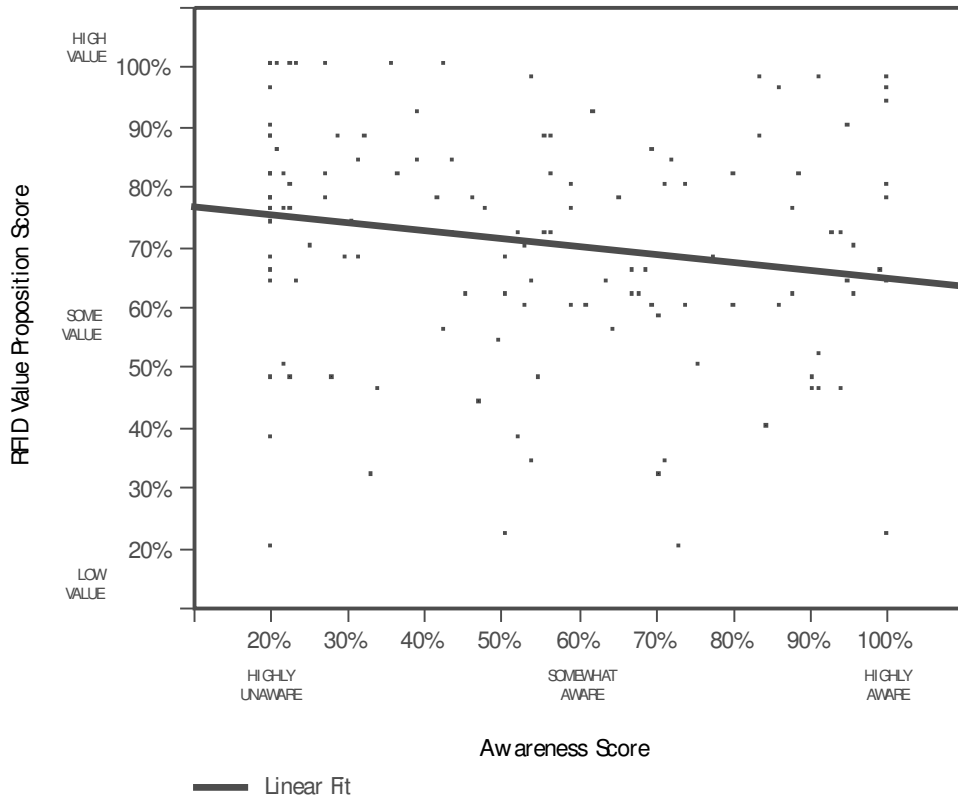


Figure 5 – Relationship between awareness and perception of RFID’s value proposition.

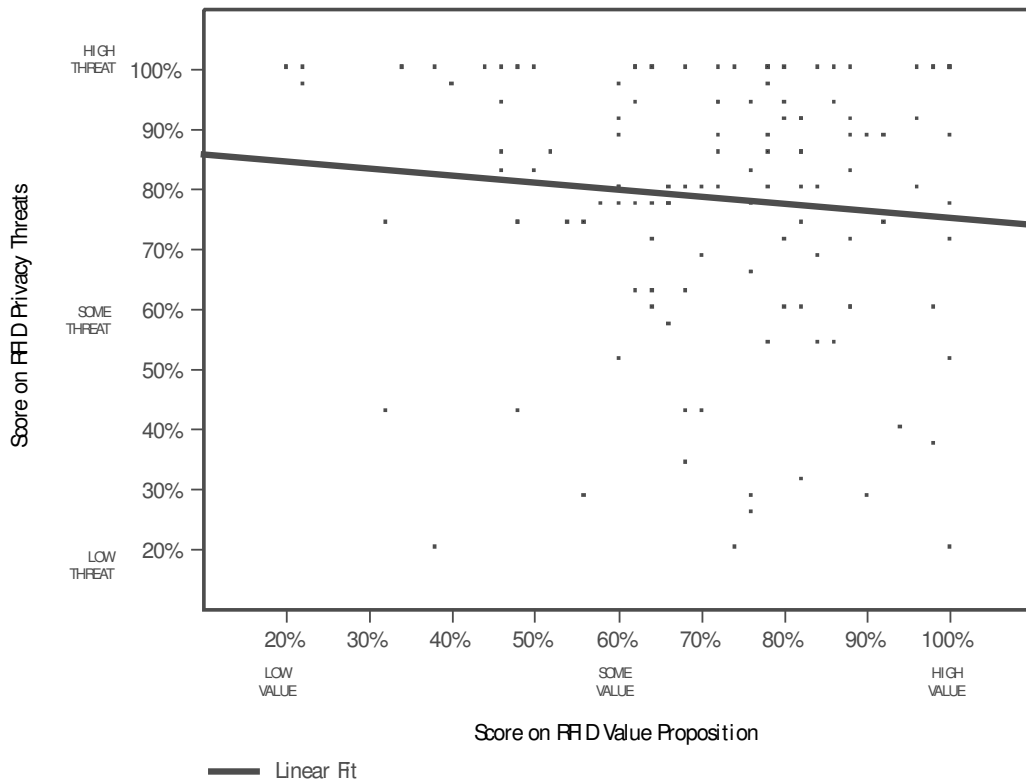


Figure 6 – Perception of RFID privacy threats in relation to perception of RFID’s value proposition.

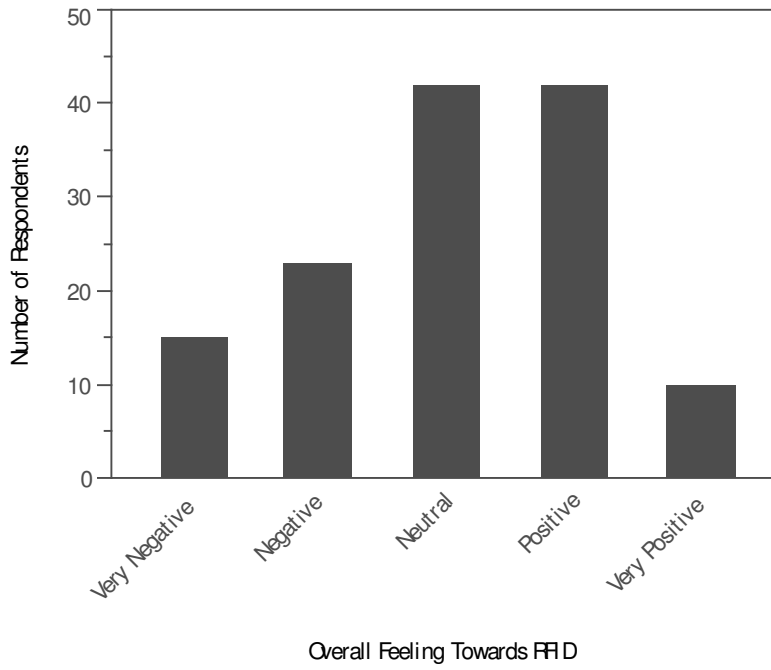


Figure 7 – Overall respondent feelings towards RFID

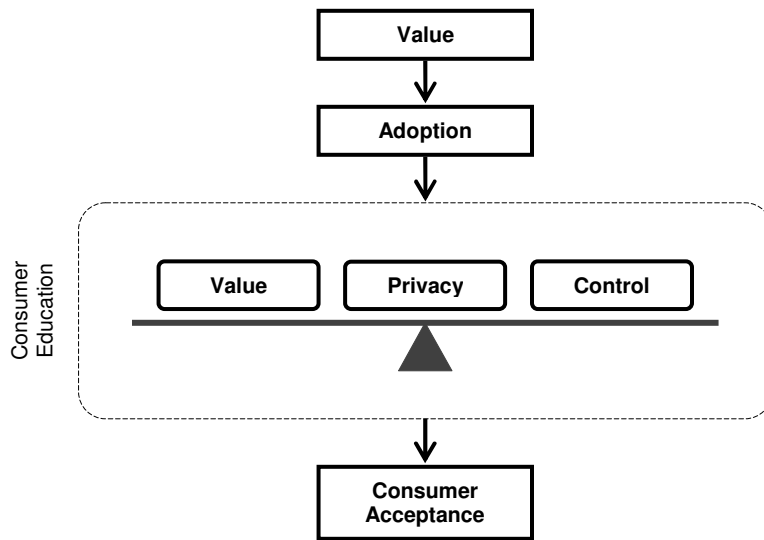


Figure 8 – Balancing value, privacy, and control through the adoption process.