Les Cahiers du GERAD ISSN: 0711–2440

RFID in Retail Environments: About Risk Perception and Attitudes

S. Blanchard

G–2005–79

October 2005

RFID in Retail Environments: About Risk Perception and Attitudes

Simon Blanchard

GERAD and HEC Montréal
3000, chemin de la Côte-Sainte-Catherine
Montréal (Québec) Canada, H3T 2A7
simon.blanchard@hec.ca

October 2005

Les Cahiers du GERAD

G–2005–79

Abstract

The use of RFID technology has received a lot of attention due to the possible infringements on information privacy rights. This paper evaluates links between risk perception and attitudes towards the technology. Precisely, it demonstrates that even though all customers perceive risks in having RFID technology in retail environments, the risk perception dimensions have different weights in predicting attitude for different groups of respondants.

Key Words: RFID, risk perception, retailing, unsupervised classification.

Résumé

L'utilisation de la technologie RFID est continuellement sujette à la controverse pour des questions de protection des renseignements personnels. Cette étude évalue le lien entre la perception du risque et le changement d'attitude envers les compagnies qui utilisent la technologie RFID dans des environnements de commerce de détail. Il est notamment démontré que l'importance des différents facteurs de risque, lorsque prédicteurs du changement d'attitude, varie selon différents sous-groupes de l'échantillon.

Acknowledgments: The author would like to thank Gilles Caporossi (GERAD) for his clusterwise linear regression program and John W. Stamey (Coastal Carolina University) for his insightful comments.

1 Introduction

RFID (Radio Frequency Identification) is a method that uses unique electronic tags on objects so that they can be tracked or identified wirelessly, using radio waves. It has gained attention in the last fifteen years, used or studied in industries such as collision warning systems (Ruff and Hession-Kunz 2001), supply chain management (Barry 2001), recycling (Saar and Thomas 2003), vehicle access control (Blythe 1999) and remote access to medical records (Hall, Vawdrey and al. 2003). Because of major advances in technology, the tags are cheaper, smaller and, as a result, possibly invisible to the eye. This enables owners of such systems to implant them nearly on anything, as well as to collect data from more sources and types than previously possible.

Groups like Customers Against Supermarket Privacy Invasion and Numbering (CASPIAN), managed to put a stop at Gillette's RFID trial (2003). Members of the groups say they represent all consumers in their claim that extensive data collection is a despiteful practice. Previous studies such as Peppers and Rogers (1997) found that consumers who do not feel in control of their personal information are not likely to be willing participants in any dialogue. As many as 80% of consumers are concerned about privacy and those are not only concerned about how the information was obtained, but also about its accuracy and with whom it is shared (Dommeyer and Gross 2003). Consumers lack knowledge about information privacy and that they even tend to exaggerate what information companies can get about them (Dommeyer and Gross 2003; Phelps, Nowak and Ferrell 2000). A study by Nowak and Phelps (1992) showed that because of this, people are less aware of the ways they can protect their privacy.

The study reported in this article contributes to the debate about the use of RFID technology in a retail environment. This paper first addresses whether all consumers perceive risks associated with the use of RFID in a retail setting. Then, it aims to verify if all consumers give equal importance to the risk perception dimensions when related to attitude towards the use of RFID. This paper extends previous research in two ways. First, the consumers' awareness of the potential intrusion into their privacy is explored, consistent with the current RFID literature. Second, the impact of RFID technology on consumer attitudes and the risk perception factors are assessed so as to gauge their relative importance in estimating attitude, for various homogenous subgroups of the sample.

This paper is structured as follows: In the following section, we give a brief introduction to RFID technology, including several well-known privacy concerns regarding the use of the technology. Then, risk perception factors are introduced and the methodology is detailed. In the third section, the results are presented.

2 Information Privacy and RFID

A simple RFID system might consist of a uniquely identified tag, a tag reader, an antenna and an inventory system. From the perspective of a RFID system, a tag is more than just a barcode. Actually, the tag does not only permit identification of a product through a Universal Product Code (UPC) or European Article Number (EAN), but it also allows authorized readers to identify a particular item. This is an equivalent to a passport number on a product. The tags can be active, which means that they have their own power sources, or passive, which means that they can draw their power from readers who send queries. Active tags are generally costlier and can be read from greater distances.

For owners of RFID systems, the possibilities for data collection are endless. And so are the possibilities for infringement of privacy, either by the owner of the RFID system or by a third-party. Imagine the following situations:

- A thief cruises the streets with a scanner looking for valuable art or electronics before they choose the best home to burgle.
- A store manager inventories all your personal items prior to entering.
- Your favorite video store sends a personalized list of recommended adult movies to your house, and your children actually receive the flyer.

A number of techniques have been proposed to ensure customer privacy against such situations. The most common techniques are the "kill-tag" feature and password protected tags. A detailed review of potential techniques is done by Weis (2003).

Privacy is now often thought of as the power to selectively reveal oneself to the world (Hugues 1993). This implies a choice, which represents the main objective of the information privacy activist movements. Previously requested to protect citizens from the "Big Brother," fair information practices are also implemented today to limit data collection from enterprises. No different from frequent shopper cards which receive extra attention because they allow collection of extensive information; RFID tags represent an important threat to information privacy (McCullagh 2003).

The threat is important enough that a European Union official committee is working on privacy guidelines for RFID (Rohde 2005). Such guidelines have already been proposed in a RFID Bill of Rights (Garfinkel 2002a). The Bill of Rights, partly based on the Code Fair Information Act of 1974, consists of five principles (Garfinkel 2002b):

1. The right to know if a products contains a RFID tag.
2. The right to have embedded tags removed, deactivated or destroyed when a product is purchased.
3. The right to have first class alternatives: consumers should not lose other rights (e.g. to return a product) if they deactivate the tag.

4. The right to know what information is stored in their RFID tags. If the information is incorrect, there must be a way to correct it.
5. The right to know when, where and why a RFID tag is being read.

3 Methodology

Risk perception factors Many different efficient methods have been proposed to measure risk perception (Mitchell 1999). In measuring risk perception for phenomena or events, psychometric factor models have proved to be useful (Sjoeberg, Moen and Rundmo 2004). Of the factors proposed by Sjoeberg (2002) seven were retained for this investigation. These factors may be thought of as representing three distinct dimensions: personal involvement, risk understanding, and benefits. They are explained briefly in Table 1.

Survey methodology A questionnaire described as a survey about RFID technology was distributed to 183 respondents. It was administered in French to students and recent graduates in the province of Quebec, Canada, through an Internet survey. The average age of the respondents is 24.28 (std. 3.24, five missing), 96 were males, 84 females and three did not indicate their gender. Before proceeding with the questions, respondents were asked to read a short page, with photographs, that introduced RFID technology. Figure 1 presents a translation of the page. The questionnaire had 25 questions on a one to five Likert scale, one meaning that the respondent strongly disagreed with the statement and five meaning that the respondent strongly agreed with the statement. A 26th question was asked using a one to five Likert scale. This time the scale representing the proclaimed change in liking that a respondent would have if a store introduced RFID technology. The 26 questions were indicators for the seven risk perception factors used and for the attitude component.

Clusterwise Linear Regression Considering a set of n observations ($i = 1...n$) with m variables ($j = 1...m$), where y is the dependant variable we want to estimate using the

Table 1: Risk perception factors

About Personal Involvement

Voluntariness: If a risk is perceived as imposed, then it is perceived as a greater risk.
Familiarity: If a risk is perceived as unfamiliar, then it is perceived as a greater risk.
Trust: If a risk is related to an organization lacking in trust, then it is perceived as a greater risk.

About Risk Understanding

Uncertainty: If a risk is perceived as having unknown consequences, then it is perceived as a greater risk.
Reversibility: If a risk is perceived as having irreversible effects, then it is perceived as a greater risk.
Understanding: If a risk is perceived as badly understood, then it is perceived as a greater risk.

Benefits: If a risk as unclear or no benefits, then it is perceived as a greater risk.

values x_{ij} matrix. The goal of clusterwise linear regression is to group observations in partitions so that the following objective function is minimized (Spaeth 1979):

$$\min \sum_{i=1}^{n} \sum_{k=1}^{K} z_{ik} \left(y_i - \sum_{j=1}^{m} b_{jk} x_{ij} + b_{0k} \right)^2$$

Subject to:

$$\begin{aligned} &\sum_{k=1}^{K} z_{ik} = 1, \quad \forall i \\ &z_{ik} \in \{0,1\} \end{aligned} \tag{1}$$

where z_{ik} is equal to one if observation i is a member of cluster k, otherwise zero. We therefore obtain different sets of regression coefficients b_{jk} for each of the K partitions that will allow us to minimize the total error when we use these regression equations for the different partitions.

Simply put, clusterwise linear regression permits the identification of classes and, at the same time, the estimation regression models for each class. In our case, a model is used to see whether homogenous subgroups give different importance to the risk perception factors in predicting their attitude.

A Variable Neighborhood Search (VNS) algorithm with an alternate local descent Because the clusterwise regression algorithm does not always provide a good solution by itself, a Variable Neighborhood Search routine was added to the previous algorithm to prevent from being stuck in a bad local optimum. The routine goes as follows (Hansen and Mladenović 2001):

Repeat the following k times or until max cpu time:

1. Shaking: Generate a new partition x' at random from the k^{th} neighborhood of x ($x' \in N'_k(x)$)
2. Exploration of Neighborhood: From x', apply a descent method and obtain x'' the new local optimum.
3. Move or not: If x'' is better than x, replace x by x'' and go back to step one. If x'' is not better than x, increase by one the number of local reassignments possible per the descent method used in step two, until it is maxed. If the number of local reassignments is maxed, then put $k = k + 1$ and reset the number of local reassignments for the descent method.

The alternate local descent method consists of reassigning observations to the partitions that they best fit, after each optimization. If at least one observation has been reassigned, then we re-optimize. Therefore, VNS actually chooses k times two clusters and reassigns randomly the observations between the two clusters. If the descent method does not find a better solution before reaching the maximum number of reassignments, k is increased by one.

4 Results

Survey questions for each factor, along with their associated Cronbach Alpha, are presented in Appendix A. With seven out of eight factors with alphas greater than 0.7, which is an acceptable rate for measuring the reliability of the generated scales (Nunnaly 1978), it is fair to say that the questionnaire has a good internal validity. Then, predictors were aggregated using the rounded average of the indicators in order to keep their original structure.

Obtaining the underlying structure Clusterwise regression was ran on the data. The attitude factor was used as the dependant variable and the seven risk perception factors were used as the independent variables. We ran the clusterwise regression model for $k = 1...9$ and we kept the objective solution value from the best solution obtained. From k=1 to 3, adding a partition reduces significantly the error of the regression equations. However, using more than three partitions does not significantly reduce the error, which lets us believe that the sample has a structure composed of three partitions. The means and standards errors of the seven factors and attitudes are presented in Table 2. Other unsupervized classification methods could not find a clear cut-off point, suggesting that there is no underlying structure when the objective is focused on inter and intra group variance.

Table 2: Factor means by cluster

	Cluster 1	n=67	**Cluster 2**	n=56	**Cluster 3**	n=60
Factor	Mean	Std	Mean	Std	Mean	Std
Voluntariness	4,30	0,798	4,46	0,738	4,32	0,833
Familiarity	2,34	0,827	2,34	0,94	2,52	1,066
Trust	4,52	0,804	4,34	0,978	4,55	0,622
Uncertainty	4,07	0,876	3,91	1,032	4,20	0,953
Reversibility	3,48	1,272	3,57	1,305	2,98	1,334
Understanding	3,94	0,903	3,77	1,095	4,05	1,080
Benefits	3,03	0,904	2,77	1,027	2,43	1,125
Attitude	3,24	0,854	3,18	1,046	2,35	1,162

Risk perception for the seven factors seems to be the same for all three clusters. The only significance between the means being between cluster two and three for reversibility (Games-Howell, Mean diff.=0.59 p-value=0.047) and between cluster one and three for benefits (Mean diff.=0.60 p-value=0.004). For each cluster and for each factor, a 1-sample t-test was done at a 95 percent confidence level. Voluntariness, familiarity, trust, uncertainty, visibility and understanding have factor means significantly different from three, but reversibility is not significant for all clusters. The benefits factor is only significantly lower than three for the third cluster.

The fact that traditional clustering method could not find an underlying structure but clusterwise linear regression could suggests that even though there are not natural groupings when considering the risk perception measurements, there are natural groupings when considering the importance that they give to each of those factors when predicting attitude.

The seven factors, when used for estimating the attitude towards RFID use in retail environment, are significant predictors in almost all cases as shown in Table 3. Even though the means of the variables are not different, the clusters have different regression coefficients. To test this, the following test was done: $H_{0ij} : \beta_{ij} - \beta_{ij} = 0$, $H_{1ij} : \beta_{ij} - \beta_{ij} \neq 0$ where β_{ij} is the regression coefficient j ($j = 1...7$) for cluster i ($i = 1...3$), for all i and j where $i \neq j$. T-values were estimated, calculating the degree of freedom for each pair without assuming equal variances. The results of these tests are presented in Appendix B. Since the degrees of freedom are larger than 30 for all possible comparison, they are omitted from the table. The table shows that even though the three clusters have quite similar risk perception, respondents from the clusters value them differently when estimating attitude.

Describing the structure To better understand and to understand consumers' attitudes towards the use of RFID in retail, it is interesting to analyze the results for each cluster separately.

Table 3: Regression coefficients by cluster

	Cluster 1				Cluster 2				Cluster 3			
	B	Std.	t-value		B	Std.	t-value		B	Std.	t-value	
(Constant)	0,54	0,53	1,02		-0,03	0,48	-0,06		9,03	0,56	16,10	*
Voluntariness	0,16	0,08	2,05	*	0,77	0,09	8,54	*	-0,82	0,07	-12,35	*
Familiarity	-0,26	0,07	-3,72	*	0,55	0,06	8,58	*	-0,23	0,05	-4,81	*
Trust	-0,12	0,08	-1,56		-0,25	0,06	-3,96	*	-0,24	0,08	-2,81	*
Uncertainty	0,79	0,08	9,58	*	-0,60	0,07	-7,95	*	0.00	0,08	0,04	
Reversibility	0,03	0,05	0,65		-0,18	0,04	-4,12	*	-0,01	0,04	-0,28	
Understanding	-0,53	0,08	-6,76	*	0,28	0,07	3,92	*	-0,42	0,08	-5,45	*
Benefits	0,63	0,07	9,32	*	0,54	0,06	9,37	*	0,10	0,06	1,73	*
Ajd. R^2	0,731				0,841				0,899			

* represents significant coefficients at a 95% confidence level

Respondents from the first cluster seem to fit the optimist type. Even though they perceive risks associated with the use of RFID, they do not know much about the technology. The negative coefficient for familiarity shows that if they were to know more about it, they would have a worse attitude. Their attitude factor score is significantly greater than three (mean=3.24, p-value=0.025) so it is fair to say that they have a somewhat positive attitude towards RFID in retail environments.

The second cluster members could be described as realists. They do not know much about the technology itself, but believe that in any case a voluntary system would help. If they were to know more about the systems and the risks and if they were shown real benefits for their participation, their attitude would be improved. Their attitude factor score is not significantly different from three (mean=3.18, p-value=0.207), so it is possible to say that they either do not care or that they do not have enough information yet.

Finally, the third cluster members can be described as technology pessimists. With all coefficients of negative signs, the more they perceive risk the less favorable is their attitude towards RFID. They see very little benefits for consumers in the implementation of such systems but that is not really a concern for them as the coefficient is not significant. It seems that information privacy is the central issue, since they strongly emphasize the importance of the voluntariness of the system. Their attitude factor score is significantly smaller than three (mean=2.35, p-value=0.000) and it is therefore safe to say that they have a negative attitude towards the implementation of such systems.

5 Conclusions, remarks and direction for further research

Risk for the use of RFID was perceived for all factors, except for reversibility. This is consistent with previous research that showed that people care about their information privacy. While there was little difference between the risk perception between respondants, the importance they give to the risk perception factors when explaining the variation in attitude varies significantly across groups. These groups have different attitude changes towards companies that use RFID in retail environments and, more importantly, the factors that can influence attitude are different.

We verified that even though customers perceive a treat to their information privacy when RFID technology is implemented in retail environments, the attitude changes are not the same. Companies and organizations that want to influence attitude should not consider all customers to be alike because different customer groups respond differently to the different risk perceptions. For future research, it would be interesting to collect more sociodemographic information in order to make more detailed profiling analyses so that companies and organizations can have a better understanding of the different groups.

Appendix A – Questions by factors and Cronbach Alphas.

Voluntariness:	Alpha: 0.72
It is important for me to be able to refuse a company to collect data on me with RFID technology.	
It is important for me to be able to stop a company from collecting additional information with RFID technology as soon as I have purchased a product.	
It is important for me to be able to know which stores use RFID-tags on their products.	
It is important for me to be able to know which products have RFID-tags.	
Familiarity:	Alpha: 0.78
I am familiar with radio wave encryption methods and their effectiveness.	
I am familiar with RFID technology in general.	
I am familiar with the Federal Privacy Act (1985).	
I am familiar with information privacy rights in my Canada.	
Trust:	Alpha: 0.74
It is important for me that the company is one that you trust.	
It is important for me to have easy access to a company policy statement indicating what data that is collected.	
It is important for me to have easy access to a company policy statement indicating who has access to the data that is collected.	
Uncertainty:	Alpha: 0.66
It is probable that some personal information is shared with companies that I did not approve.	
It is probable that someone hacks the system (i.e. gets the signal waves) and then uses some of my personal information against me.	
The spread of personal information to unauthorized people would bring me discomfort.	
Reversibility:	Alpha: 0.88
Assuming that some personal information was given to a third party without my approval, I will be able to find who let the information spread out.	
I will be able to get compensated if some of my personal information gets stolen/inappropriately shared.	
Understanding:	Alpha: 0.83
It is likely that a company uses personal information in a way that brings me discomfort.	
It is likely that a company collects personal information that I did not explicitly agree to give.	
Benefits:	Alpha: 0.73
Companies that use RFID on their products will save me time by offering me products that correspond better to my needs.	
Companies that use RFID-tags on their products will be able to identify theft and fraud more easily, thus resulting in a decrease in product prices for customers like me.	
In general, customers like me will benefit from having RFID technology used at their favorite stores.	
Attitude towards RFID:	Alpha: 0.88
I am in favor of the adoption of RFID technology the supermarkets I visit.	
I am in favor of the adoption of RFID technology the department stores I visit.	
I am in favor of the adoption of RFID technology the drugstores I visit.	
What opinion would you have towards a company who adopts the RFID technology? (1 means you would like the company a lot less while 5 means you would like the company a lot more.)	

Appendix B – Comparison of regression coefficients between clusters

T-value obs.	1 and 2		1 and 3		2 and 3	
Voluntariness	-28,97	*	59,90	*	77,73	*
Familiarity	-48,70	*	-2,05	*	53,52	*
Trust	7,75	*	6,57	*	-0,68	
Uncertainty	70,85	*	43,64	*	-31,68	*
Reversibility	18,61	*	4,25	*	-16,41	*
Understanding	-43,56	*	-6.00	*	37,76	*
Benefits	5,79	*	37,95	*	31,12	*

* indicates a significant difference at the 95% confidence level

Appendix C – Survey introduction page

INTRODUCTION
Radio frequency identification (RFID) is a method of remotely storing and retrieving data using devices called RFID tags. An RFID tag is a small object, such as an adhesive sticker, like this one, that can be attached to or incorporated into a product.

(picture of a tag) (picture of a jacket which has a RFID pocket, which clearly advertises the tag)

Each chip has a unique identification number. If you put a RFID chip on a CD instead of a bar code, for example, it means that you can identify that particular CD uniquely. It's like a passport number.

In the jacket picture, the tag is inside a little pocket and clearly advertised. However, tags can be made to be almost invisible to the eye.

RFID tags contain antennas to enable them to receive and respond to radio-frequency queries from an RFID transceiver. A RFID receiver can look like this:
(picture of a reader)

A reader can be similar to this one or be in a machine in a very similar way to that of the barcode readers in the supermarkets. It can also be put on shelves to monitor when an item is taken out of the shelves, for example.

RFID tags have been used in various industries:
- for garage doors to detect objects
- to automate toll payment
- to identify clothes and other retail products.
- to identify employees, patients, customers.

A RFID System is connected to a database where various data is collected and stored.

References

Barry, C. 2001. RFID Tracks Packages, 'Speaks' to Consumers. *Food and Drug Packaging*, 53–56.

Blythe, P.T. 1999. RFID for road tolling, road-use pricing and vehicle access control. *IEE Colloquium on RFID Technology, London, October 1999.* 8/1-8/16.

Caporossi, G., D. Alamargot, D. Chesnet. 2004. Using the computer to study the dynamics of handwriting processes. *Lecture Notes in Computer Science*, 3245, 242–254.

Caporossi, G., P. Hansen. 2005. A Least Squares Clusterwise Regression Heuristic Using Variable Neighborhood Search. *Les Cahiers du GERAD*, G–2005–61, Technical Report.

Capsian. 2003. Gillette Reverses Position on RFID Spy Chips at Mach 3 Speed. Caspian Press Release, (Accessed April 19th 2005) http://www.nocards.org/press/pressrelease 08-19-03.shtml.

Dommeyer, C.J., Gross B.L. 2003. What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing* 17 (Issue 2), 34–51.

Garfinkel, S. 2002a. An RFID Bill of Rights, *Technology Review* (October).

Garfinkel, S. 2002b. Adopting Fair Information Practices to Low Cost RFID Systems, *Privacy in Ubiquitous Computing Workshop, Sweeden, 2002.*

Hall, E.S., D.K. Vawdrey, C.D. Knuston, J. Karchibald. 2003. Enabling remote access to personal electronic medical records, *IEEE Engineering in medicine and Biology* 22, 133–139.

Hansen, P., N. Mladenović. 2001. Variable Neighborhood Search: Principles and Applications, *European Journal of Operational Research* 130, 449–467.

Hugues, E. 1993. A cyberpunk Manifesto (Accessed April 25th 2005) http://www.activism.net/cypherpunk/manifesto.html

Jacoby, J., L. Kaplan. 1972. The Components of Perceived Risk, *Advances in Consumer Research*, 3, 382–383.

Lederer, S.M., J. Mankoff, A.K. Dey. 2003. Towards a Deconstruction of the Privacy Space. *Privacy in Ubiquitous Computing Workshop, 2003.*

McCullagh, D. 2003. RFID tags: Big Brother in small packages. (Accessed April 19th 2005), http://news.com.com/2010-1069-980325.html

Mitchell, V.W. 1999. Consumer Perceived Risk: Conceptualisations and Models. *European Journal of Marketing*, 33 (1/2), 163–195.

Nowak, G., J. Phelps. 1992. Understanding Privacy Concerns: An Assessment of Consumers Information-Related Knowledge and Beliefs. *Journal of Direct Marketing* 6 (4), 28–39.

Nunnaly, J. 1978. *Psychometric theory.* New York: McGraw-Hill.

Peppers, D., M. Rogers. 1997. *Enterprise One to One.* New York: Doubleday.

Phelps, J., G. Nowak, E. Ferrell. 2000. Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing* 19, 27–41.

Rohde, L. 2005. EU offers privacy guidelines for RFID. The Industry Standard. (Accessed April 19th 2005) http://www.thestandard.com/internetnews/000996.php

Ruff, T.M., D. Hession-Kunz. 2001. Application of Radio-Frequency Identification Systems to Collision Avoidance in Metal/NonmetalMines. *IEEE Transactions on industry applications*, 37, 112–116.

Saar, S., V. Thomas. 2003. Toward Trash That Thinks: Product Tags for Environmental Management. *Journal of Industrial Ecology* 6, 133–146.

Sjoeberg, L. 2002. Factors in risk perception. *Risk Analysis* 20, 1–11.

Sjoeberg, L., B.E. Moen, T. Rundmo. 2004. Explaining Risk Perception: An evaluation of the psychometric paradigm in risk perception research. *Rotunde*, 84, Trondheim.

Spaeth, H. 1979. Clusterwise Linear Regression. *Computing* 22, 367–373.

Wedel, M., W.A. Kamakura. 1998. *Market Segmentation: Concepts and Methodological Foundations.* Kluwer Acamedic Publishers: Boston.

Weis, S.A. 2003. Security and Privacy in Radio-Frequency Identification Devices. *International Conference on Security in Pervasive Computing, Germany*, 2003.