Between Extreme Rejection and Cautious Acceptance: Consumers' Reactions to RFID-Based IS in Retail

Matthias Rothensee and Sarah Spiekermann

Social Science Computer Review 2008 26: 75 originally published online 3 December 2007
DOI: 10.1177/0894439307307687

Social Science Computer Review
Volume 26 Number 1
February 2008 75-86

10.1177/0894439307307687
http://ssc.sagepub.com
hosted at
http://online.sagepub.com

Between Extreme Rejection and Cautious Acceptance

Consumers' Reactions to RFID-Based IS in Retail

Matthias Rothensee
Sarah Spiekermann
Humboldt University, Berlin, Germany

RFID (radio frequency identification) is one of the most important technologies underlying ambient intelligence. It will enable myriad information services on retailers' shop floors and after sale. However, embedding chips in everyday products has stirred a considerable debate about people's privacy. So far it is unclear what the attitudes toward privacy in ambient intelligence are and whether they will affect the reputation of the retailer and acceptance of RFID-based information services. This article presents two empirical studies with 642 participants who saw an introductory film and subsequently evaluated the technology and potential privacy protection mechanisms. Results show that people are moderately privacy aware and that their privacy awareness is negatively related to their acceptance of the service. A group of "extreme rejecters" is identified, which hold highly negative attitudes toward RFID and significantly bias group means. The characteristics of this group are explored and privacy protection measures are evaluated.

Keywords: *ambient intelligence; privacy enhancing technology; retail; reputation; RFID*

Radio frequency identification (RFID) is a technology strongly debated in the information systems world. Next to other wireless technologies like Bluetooth or Wireless LAN it represents a major building block of the "intelligent infrastructure" or "ubiquitous computing environment" envisioned by IS researchers (Weiser, 1991). RFID allows product information to be read out from chips embedded in each everyday object, simultaneously, through optical barriers and from a distance. A strong driver of RFID adoption is its current deployment in worldwide retail and logistics operations. Major players like Wal-Mart, the Metro Group, or the U.S. Department of Defense have set ambitious roadmaps for tagging products with RFID chips. The goals are to increase efficiency and the control of supply chains, reduce counterfeits, decrease loss and waste of objects, and so on. In addition, new information systems and business models are being developed for RFID use beyond supply chain application. Here, new forms of recycling, warranty management, intelligent home applications, and infotainment systems have been discussed (Park, Won, Lee, & Kim, 2003). In particular, retailer operations are planned to be enhanced. New IS on the shop floor, personalization of offerings, and increased cashier efficiency are envisioned.

Authors' Note: Please address correspondence to Matthias Rothensee, Institute of Engineering Psychology, Humboldt University, Rudower Chaussee 18, 12489 Berlin, Germany; e-mail: rothensee@wiwi.hu-berlin.de.

Despite these ambitious plans around the RFID rollout, privacy rights organizations and researchers warn that products that embed a "communicating" chip could easily lead to privacy problems. Without doubt, with RFID technology the data that can be collected from a person increases in quantity and quality (Ackerman, 2004). Individual belongings could be scanned from a distance, personal movement tracks could be established, social networks could be built. Moreover, because of a unique electronic product code (EPC) embedded in each product, responsibility for the object's whereabouts could be created for object owners because they can be unambiguously associated with the product (Spiekermann & Ziekow, 2005).

As a result, retailers face a dilemma: On one side, an introduction of RFID services can reduce consumer purchase risks through enhanced product information, augment the shopping experience, and thus potentially promote shopping. On the other side, consumer privacy fears and potential breaches could negatively influence a retailer's reputation in the eyes of the customer (Fusaro, 2004). How can retailers address this dilemma?

There are two main groups of countermeasures for retailers to tackle the privacy problem. Technical solutions, so-called privacy enhancing technologies (PETs) restrict the possibility to read out RFID-chips, that is, with the help of a password protection scheme (Spiekermann & Berthold, 2004) or a kill signal (Chai, 2003). The second group are self-imposed privacy policies that can be used by retailers to signal their adherence to privacy principles, that is, through seals of approval (e.g., the TRUSTe web trustability certificate) or other "information policies." In addition, legislation may be created around RFID deployments in the retail sector. Few insights exist into how people evaluate these different pathways to the protection of their privacy.

Furthermore, it is not clear if privacy awareness varies by type of information, like personal (e.g., postal address) or profile information (e.g., hobbies). It has been shown already that these types of information are perceived differently (Ackerman, Cranor, & Reagle, 1999). Therefore, it is possible that violations of privacy regarding one type of data have more serious consequences than violations of another.

Considering these gaps in research, the primary questions of the current work are (a) To what extent are people privacy aware? Is their privacy awareness related to the evaluation of RFID-based IS? How do people evaluate different means to protect their privacy? And how does it affect the evaluation of the retailer when learning about privacy-evasive RFID services?

To answer these questions, two studies have been conducted. Initially, Study 1 aimed at exploring people's attitudes toward RFID-based IS, their judged sensitivity of distinct types of information and privacy protection. Study 2 employed a between-subjects design to experimentally investigate evaluations of two distinct privacy protection measures and retailer reputation.

Study 1

Method

Participants

Study 1 was conducted with 336 participants in one metropolitan (n = 185) and one rural (n = 151) area in Germany. The sample was drawn by a marketing agency and by age,

gender, education, and income matched the general German population (age: Median = 30-39 years; 52.4% female; college degree or higher: 51.2%; income/year: Median = 20,001-30,000€).

Procedure

Participants were invited to hotels in groups for a single session. They were introduced to RFID technology and application scenarios by help of professionally produced introductory films. Afterwards they were asked to fill in questionnaires about their evaluation of RFID-IS. The films, containing no music and balancing the number of positive and critical messages, aimed at giving a neutral introduction to provide participants with a common knowledge base on which they were to make their evaluations.

Stimulus

The stimulus film focused on RFID services in the retail and after-sales consumer household context (length: 6 min 22 s). It was judged rather uncritical vis-á-vis RFID technology (M = 8.84, SD=2.33; on an 11-point scale from *very critical* to *very uncritical*).

Measures

Generally, if not otherwise specified, items were formatted as 5-point Likert-type scales asking participants to judge their agreement with statements in the range of 1 (*completely disagree*) to 5 (*completely agree*).

Privacy awareness. People were asked about their attitudes toward privacy ("To me it is irrelevant if somebody knows what I buy for my daily needs," "Generally I want to disclose the least amount of data about myself"). These two items were self-developed based on statements from focus groups that were conducted in preparation of the empirical investigation presented here.

Data sensitivity. Moreover, participants were asked to assess the sensitivity of nine types of data when registering for a loyalty card program: name, postal address, e-mail address, telephone number, hobbies, profession, favorite meals, favorite holiday destinations, income, and age. Ratings ranged from 1(*not at all sensitive*) to 5 (*extremely sensitive*).

RFID acceptance. Participants judged their likely acceptance of RFID-IS by three items from technology acceptance research (Venkatesh & Davis, 2000) that were adapted to fit the present context ("I would refuse to use RFID-enabled information services," "I would naturally accept RFID-based information services," "I would use RFID-based information services"). The acceptance scale exhibited a high internal consistency (α = .84).

Emotional reactions. It has been shown that emotional reactions are determinants of information technology (IT) usage (Zhang & Li, 2004). Therefore, participants judged their emotional reactions in general when imagining to shop in the supermarket of the future on three 9-point semantic differential items (*happy/unhappy, satisfied/dissatisfied, contented/sad*), adapted from (Mehrabian & Russell, 1974). This scale also proved reliable (α = .93).

Effectiveness of legal privacy protection. Participants were asked if they believed that legal regulations would bring about a sufficient level of protection from privacy fraud.

Results

A factor analysis was conducted on the sensitivity of nine types of data. Applying the Kaiser eigenvalue criterion to the varimax rotated solution clearly suggested two underlying factors, namely Sensitivity of Personal Data (with name, postal address, e-mail address, telephone number) as opposed to Profile Data (hobbies, favorite meals, holiday destinations, profession, age, income) accounting for 64% of the total variance.[1] Factor scores of these two factors were taken as measures of the sensitivity of personal and profile data, respectively. Table 1 provides Pearson product–moment correlation coefficients of the answers to the privacy awareness questions with the sensitivity of personal and profile data. It was decided to collapse those items, yielding a single factor of Privacy Awareness with a satisfying internal consistency for exploratory research ($\alpha = .67$). People judged themselves being moderately privacy aware ($M = 3.36$, $SD = .78$).

Privacy awareness and RFID-IS acceptance. The compound measure of privacy awareness correlated $r = -.404$ ($p < .01$) with the intention to use RFID-IS. The immediate emotional reaction when imagining to shop in the RFID supermarket correlated $r = -.393$ ($p < .01$) with privacy awareness. The average reactions of participants go slightly in the direction of positive intention to use ($M = 3.19$, $SD = .97$) and positive emotional reactions ($M = 5.37$, $SD = 2.18$).

Effectiveness of legal privacy protection. Finally, participants tended to expect that legal regulations will bring about sufficient privacy protection ($M = 3.36$, $SD = 1.39$).

Discussion

In this first study we were able to demonstrate that rated sensitivities of distinct types of information are grouped into two categories, namely profile and personal data. These are equally related to privacy awareness and together form a broad but generally useful measurement instrument for Privacy Awareness. The correlations suggest that no matter what kind of data are used by retailers, violations of privacy can lead to growing privacy awareness, eventually complicating RFID-IS introduction.

It is interesting to note that as opposed to Ackerman et al. (1999) in our study e-mail address was evaluated similar to postal address and telephone number. Apparently, within the past decade e-mail has become so important that nowadays the e-mail address is regarded as personal information and considered just as vulnerable to privacy fraud as the other personal data types.

Furthermore, results show that the extent to which people view their privacy protection critical has an influence on how much they would be willing to accept RFID-based IS. In the same way, expected emotional reactions to shopping in the future supermarket are negatively related to how much people value their privacy. These results clearly show that privacy protection must be an essential element of the RFID rollout. It is nothing that customers do perceive as outdated or do not credit importance in ambient intelligence. The

Table 1
Privacy Awareness and Sensitivity of Personal and Profile Data

	Study 1			
EVERYTHING IN THIS COLUMN A FACTOR	SENSPERS	SENSPROF	PRIV1	PRIV2
FACTOR: sensitivity of personal data (SENSPERS)		.297**	.217**	–.375**
FACTOR: sensitivity of profile data (SENSPROF)			.381**	–.343**
"To me it is irrelevant if somebody knows what I buy for my daily needs." (PRIV1)				–.436**
"Generally I want to disclose the least amount of data about myself." (PRIV2)				
	Study 2			
	SENSPERS	SENSPROF	PRIV1	PRIV2
FACTOR: sensitivity of personal data (SENSPERS)		.142*	.249**	–.258**
FACTOR: sensitivity of profile data (SENSPROF)			.361**	–.340**
To me it is irrelevant if somebody knows what I buy for my daily needs (PRIV1)				–.396**
Generally I want to disclose the least amount of data about myself (PRIV2)				

*$p < .05$. **$p < .01$.

privacy problem, in fact, influences people's very decision whether to use a service or not. The results call for an adaptive privacy management approach (e.g., based on a P3P (Platform for Privacy Preferences) equivalent; Cranor et al., 2006): People with high privacy awareness should be frequently reassured that their privacy is secured, whereas less concerned people should be left to inform themselves if they desire.

As mentioned earlier several means to protect privacy can be imagined. Therefore, an important question is whether different precautions undertaken can possibly influence people's evaluation of the services in general. This question is particularly informative for the retailers to estimate the likely pay-off of engaging more in the one or the other strategy to alleviate consumers' privacy fears. Therefore, a second study was conducted, in which participant's information about how their privacy will be protected was experimentally varied. Participants were asked for the retailer's reputation to estimate the direct effect of the retailer's privacy protection strategy on this important appraisal.

Study 2

Method

Participants

Three hundred and six people from four metropolitan regions participated in the second study. The sample was drawn by a marketing agency and again matched the general German population in relevant demographic characteristics (age: Median = 30 – 39 years, 50.3% female, college degree or higher: 59%, income/year: Median = 20.001 – 30.000€).

Procedure

In Study 2, a similar procedure was used as in Study 1 except for the experimental variation of privacy protection measures: Participants were randomly split into two groups (PET: $n = 208$ and information policy: $n = 98$) which were run individually. These two groups saw slightly different film clips prior to answering the questions.

Stimulus

A general introductory film on RFID in retail was used (length: 7 min 24 s). Two versions of this film mentioned distinct privacy protection measures: The film stimulus PET explained password protection of RFID chips as a technical means to secure access to data on the chip, whereas information policy explained that the retailer will extensively inform customers about how RFID is employed in the supermarket. The film versions differed only in the information given by the speaker, not in the pictures shown. The segment containing the varied information was 40 s in length. The Study 2 stimulus was judged more critical vis-á-vis RFID than the Study 1 stimulus ($M = 7.42$, $SD = 2.59$, mean of both subgroups, no significant difference between groups PET and information policy).

Measures

The measures of RFID-IS acceptance and emotional reactions resembled those of Study 1 and again proved reliable in terms of internal consistency (acceptance: $\alpha = 85$, emotions: $\alpha = .92$). In addition to the effectiveness of legal privacy protection, participants were asked whether they generally expected retailer's privacy protection measures to be effective.

Retailer reputation. Furthermore, participants answered six questions about their perceived reputation of the general retailer (a scale taken from Bearden & Netemeyer, 1999; "The retailer is really committed to satisfy me," "If the retailer tells something about his products, it is likely to be the truth," "I think some of the statements of the retailer are usually positively biased," "The retailer is very reliable," "The retailer would do anything to make me happy," and "I know what I can expect from the retailer"). These questions were answered twice: before the film stimulus and after it. The items yielded a satisfying internal consistency (before: $\alpha = .70$, after: $\alpha = .78$). The construct was selected based on the idea that retailer reputation could be a behavior-relevant proxy for positive shopping decisions once RFID is in use (Jarvenpaa, Tractinsky, & Vitale, 2000).

Covariates. Participants were asked about their evaluation of new technology in terms of the number of jobs (diminish vs. increase) and simplification of daily life (simplify vs. complicate) with a single item each. Moreover, they judged their personal proficiency in handling everyday technology based on a 6-item scale (Beier, 1999). This scale was also internally consistent ($\alpha = .80$).

Results

Privacy Awareness

Again, a factor analysis conducted in the same way as in Study 1 revealed that variance in the data sensitivity items could be explained by the underlying factors of Sensitivity of

Table 2
"Extreme Rejecter's" (Ext) Characteristics in Contrast to the Rest of the Sample (Non-Ext)

	M_{Ext}	$M_{Non\text{-}Ext}$	t^a	df	Significance
Number of jobs	4.57	4.01	3.48	297	$p < .01$
Simplification of life	3.00	2.42	3.84	296	$p < .01$
Privacy awareness	4.08	3.32	6.32	304	$p < .01$
Technological proficiency	3.25	3.68	–2.92	304	$p < .01$
Legal regulations	3.87	4.08	1.37	303	$p = .17$
Retailer engagement	1.54	2.39	–5.07	304	$p < .01$

a. Independent samples *t* test for equality of means.

Personal and Profile Data. These factors made up 62% of the total variance and again correlated moderately with the items measuring privacy awareness (Table 1). Thus, data sensitivity factors and privacy awareness items were collated, yielding a single factor of Privacy Awareness with a satisfying internal consistency ($\alpha = .62$). Again, people judged themselves moderately privacy aware ($M = 3.44$, $SD = .80$).

Privacy Awareness and RFID-IS Acceptance: Extreme Rejecters

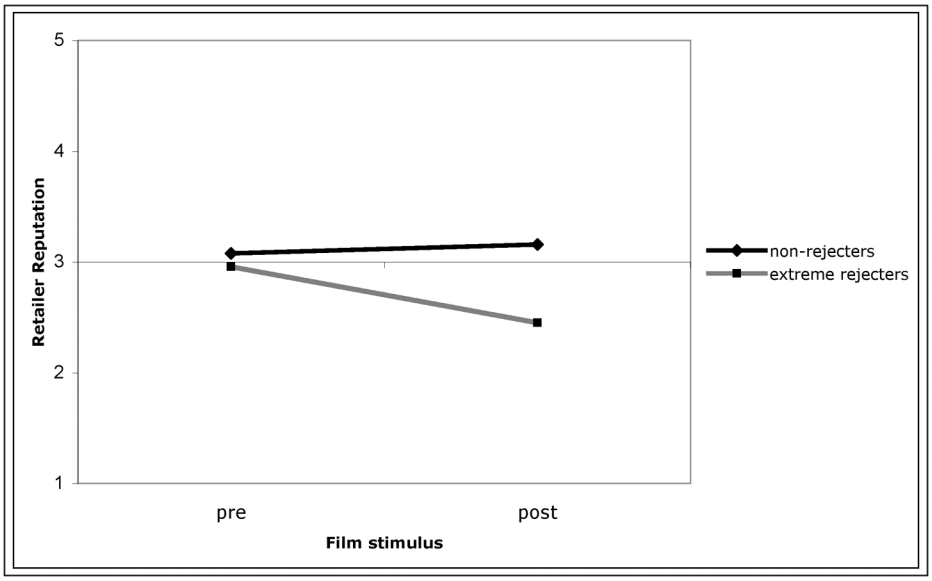
Participants' predictions of their RFID-IS acceptance were less optimistic than in Study 1 ($M = 2.69$, $SD = 1.16$), so were their emotional reactions when shopping in the supermarket of the future ($M = 4.35$, $SD = 2.03$). Averaged reactions, however, were strongly biased by a group of people ($n = 46$) who could be labeled "extreme rejecters": These participants answered any question pertaining to expected RFID-IS acceptance with the most extreme negative answer possible. This is a particularly astounding result given that these people were drawn randomly from the German general population and distributed almost evenly over four metropolitan areas across the country. This group of people exhibited several distinguishing characteristics (see Table 2): They are more critical in the evaluation of new technologies in terms of the number of jobs and of the simplification of daily life. They are more privacy aware and report lower levels of technical proficiency. There was no concentration around a particular demographic group, the number of members was equal for both sexes. The correlations between privacy awareness and RFID-IS acceptance ($r = –.467$, $p < .01$), and emotional reactions ($r = –.427$, $p < .01$) mirrored the pattern obtained in Study 1.

Privacy Awareness and Retailer Reputation

On average, people's evaluation of the reputation of the retailer did not degrade after having learned about RFID ($M_{pre} = 3.05$, $M_{post} = 3.05$). This, however, depends on privacy awareness ($r = .268$, $p < .01$). A median split of privacy awareness revealed that for less privacy aware participants retailer reputation increased after the film, whereas the more privacy aware participants became even more critical in their evaluation of the retailer ($t = 3.91$, $df = 303$, $p < .01$).

Furthermore, membership in the group of extreme rejecters interacts with reaction to the film in terms of retailer reputation: While the nonextremists hardly react to the film at all, extreme rejecters react strongly negatively (see Figure 1).

Figure 1
Retailer Reputation Before and After the Film Stimulus for Extreme Rejecters Subsample and All Other Participants



Privacy Protection Measures and RFID-IS Acceptance

It was investigated whether information about different privacy protection measures (privacy enhancing technology vs. information policy) resulted in differences of RFID-IS acceptance. This was not the case, experimental groups did not differ in their RFID-IS acceptance (PET: $M = 2.56$, info: $M = 2.60$, $t = –.31$, $df = 304$, $p = .753$). Neither did they differ in terms of their emotional reaction (PET: $M = 4.33$, info: $M = 4.41$, $t = –.34$, $df = 304$, $p = .733$).

Effectiveness of Privacy Protecting Measures

Finally, as in Study 1, participants expected that legal regulations will bring about sufficient privacy protection ($M = 4.05$, $SD = .98$). There were no significant differences among the experimental groups regarding their evaluation. They doubted, however, that retail industry will engage sufficiently in privacy protection ($M = 2.26$, $SD = 1.09$). It is interesting to note that participants were less pessimistic when they were given information about retailer's information policy ($M = 2.63$, $SD = 1.13$) than when informed about RFID chips' password protection ($M = 2.09$, $SD = 1.02$).

The group of extreme rejecters answered the question pertaining to privacy protection from the retailer significantly more skeptical, than the nonextreme (see Table 2). They did not differ from the rest of the sample in their evaluation of legal privacy regulations, which were uniformly regarded effective.

General Discussion

Even though privacy is a major research area in computer science these days, engineering and other disciplines say that, "we have little idea of the ways in which people in their ordinary lives conceive of privacy and their reactions to the collection and use of personal information" (Hine, 1998, p. 255). The current study aimed to address this gap by directly asking people about their attitudes toward RFID-based IS in the future and relating those to their privacy awareness.

The results obtained in the two studies clearly point to one direction: Customers are aware of the privacy problems that become salient with the introduction of information-rich RFID-based services. Their tentative evaluation of such services, however, is basically neutral. Our analysis shows, however, that privacy awareness is negatively related to emotional appreciation and to acceptance of the services in both studies. This means that when retailers clarify that they value customers' privacy, people will trust the technology more and will be more likely to adopt it. It has to be noted, however, that according to the results regarding the effectiveness of retailer's privacy protection measures, retailers rather have the potential to avoid negative attitudes than to create favorable ones. It is possible that active privacy protection is something like a basic requirement, a condition sine qua non that has to be fulfilled before considering enhancing people's attitudes by increasing perceived usefulness (by adding functionality, ease of use, personalization, adaptivity, etc.).

Clearly, our results do not permit causal inferences on the dynamics of privacy awareness and RFID-IS acceptance. One scenario could be that if people learn about new RFID-IS and come to like them, they will become more liberal in terms of privacy. It could also be that circumstances that render a person more privacy aware, like intrusions into other domains (e.g., massive e-mail spam) render the person more cautious when it comes to RFID-based IS. Furthermore, it is possible that privacy awareness works as a moderator of the relationship between organizational privacy policy and consumer acceptance of RFID-IS. It is an important question for further research to experimentally disentangle cause and effect to identify the relevant strategy for the introduction of such systems.

Other studies (Cranor, Reagle, & Ackerman, 1999; P&AB, 2003; Spiekermann, Grossklags, & Berendt, 2001; Westin, 1991) have shown that there are interindividual differences, such that people can be represented on a continuum between "privacy fundamentalist" and "generally unconcerned." This fact has been confirmed in our study. It remains an open question, however, on what these differences depend exactly. Probably privacy awareness is best conceptualized as a generalized and stable attitude that people acquire based on repeated experiences; and, therefore, it is the counterpart of trust in the retailer (Jarvenpaa et al., 2000). As Shneiderman (2004) described it, "trust is difficult to generate, easily shaken, and once shaken extremely difficult to rebuild" (p. 150). Assuming the same dynamics for privacy awareness, it would suggest to advise retailers to adopt a conservative privacy protection approach—this might be better than increasing privacy awareness and thereby diminishing people's RFID acceptance by a single catastrophic privacy breach. Whether there is a relationship between trust in the retailer and privacy awareness, however, is a question to be answered by further research.

A segment of 15% of participants could be labelled "extreme rejecters" based on their answers to the questions pertaining to acceptance of RFID-IS. This group will deeply oppose the introduction of RFID-IS in future supermarkets. Whether the strict rejection of RFID-IS will translate into actual behavior or will merely be a lip service paid in the absence of personal experience is another valuable goal for further research. It has been shown that people, in the majority of cases, behave consistently with their attitudes (Sheppard, Hartwick, & Warshaw, 1988), even though in the context of privacy preferences the opposite has also been found (Berendt, Guenther, & Spiekermann, 2005). Campaigns like Boycott Benetton (Batista, 2003) impressively demonstrated the disruptive potential of rejecter's movements against introduction of RFID tags and have to be taken seriously.

It is interesting to note that the group of extreme rejecters equally believed legal regulations to be effective in protection of their privacy. On the other hand, they were more skeptical concerning the protection offered by retailers, a hint to the fact that the rejectance indeed aims specifically at the commercial entity. It would be worthwhile to investigate whether such a segment exists in other countries as well.

To alleviate customer fears about RFID it is necessary to introduce effective data protection measures, especially through active information policies. Technical solutions (Floerkemeier & Schneider, 2004; Langheinrich, 2002) can only succeed if they are easy to understand (Rogers, 2003) and they generally seem to be less accepted in the first place. There are many ways in which customers can be protected from privacy intrusions, just as there are many ways in which someone's privacy can be intruded on (Spiekermann & Ziekow, 2006). If people get the feeling of losing control over their data through the introduction of RFID (Spiekermann, 2005), they will be inclined to show reactance (Brehm, 1966) toward industry's efforts to persuade them with sugar-coated messages. Therefore, a combined effort of legal enforcement, organizational policies, and technical solutions seems to be the most promising strategy for privacy protection in an RFID-IS world. Obviously, people expect legal regulations to effectively protect their privacy but still mistrust of the industry remains with the same to provide effective privacy responsibility.

Note

1. The rotated factor solutions are omitted for the sake of brevity. They can be retrieved on request from the corresponding author.

References

Ackerman, M. S. (2004). Privacy in pervasive environments: Next generation labelling protocols. *Personal and Ubiquitous Computing, 8*(6), 430-439.

Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999, November). *Privacy in e-commerce: Examining user scenarios and privacy preferences.* Paper presented at the 1st ACM Conference on Electronic Commerce, Denver, CO.

Batista, E. (2003). *"Step back" for wireless ID tech?* Retrieved May 31, 2007, from `http://www.wired.com/gadgets/wireless/news/2003/04/58385`.

Bearden, W. O., & Netemeyer, R. G. (1999). Handbook of marketing scales—Multi-item measures for marketing and consumer behavior research. Thousand Oaks, CA: Sage.

Beier, G. (1999). Kontrollueberzeugungen im Umgang mit Technik [Control beliefs in exposure to technology]. *Report Psychologie, 24*(9), 684-693.

Berendt, B., Guenther, O., & Spiekermann, S. (2005). Privacy in e-commerce: Stated preferences vs. actual behavior. *Communications of the ACM, 48*(3), 38-47.

Brehm, J. W. (1966). *A theory of psychological reactance*. New York: Academic Press.

Chai, W. (2003). *Philips adds "off switch" to RFID tags*. Retrieved January 14, 2007, from `http://news.zdnet.co.uk/itmanagement/0,1000000308,2134292,00.htm`.

Cranor, L. F., Hogben, G., Langheinrich, M., Marchiori, M., Presler-Marshall, M., Reagle, J., et al. (2006). *The Platform for Privacy Preferences 1.1 (P3P1.1) Specification*. Retrieved May 31, 2007, from `http://www.w3.org/tr/p3p11/`.

Cranor, L. F., Reagle, J., & Ackerman, M. S. (1999). *Beyond concern: Understanding net users' attitudes about online privacy.* (Technical Report No. TR 99.4.3). Denver, CO: AT&T.

Floerkemeier, C., & Schneider, R. (2004, November). *Scanning with a purpose—Supporting the Fair Information Principles in RFID protocols.* Paper presented at the Ubiquitous Computing Systems. Revised selected papers from the 2nd International Symposium on Ubiquitous Computing Systems, Tokyo, Japan.

Fusaro, R. (2004, December). None of our business. *Harvard Business Review*, 33-44.

Hine, C. (1998). Privacy in the marketplace. *Information Society, 14*(4), 253-262.

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information Technology and Management, 1*(1/2), 45-71.

Langheinrich, M. (2002, October). *A privacy awareness system for ubiquitous computing environments.* Paper presented at the 4th International Conference on Ubiquitous Computing, Heidelberg, Germany.

Mehrabian, A., & Russell, J. A. (1974). *An approach to environmental psychology*. Cambridge, MA: MIT Press.

P&AB. (2003). Consumer privacy attitudes: A major shift since 2000 and why. *Privacy & American Business Newsletter, 1ß*(6), 23.

Park, S. H., Won, S. H., Lee, J. B., & Kim, S. W. (2003). Smart home—Digitally engineered domestic life. *Personal and Ubiquitous Computing, 7*(3/4), 189-196.

Rogers, E. M. (2003). *Diffusion of innovations.* New York: Free Press.

Sheppard, B. H., Hartwick, J., & Warshaw, P. R. (1988). The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. *Journal of Consumer Research, 15*(3), 325-343.

Shneiderman, B. (2004). Leonardos laptop. Human needs and the new computing technologies. Cambridge, MA: MIT Press.

Spiekermann, S. (2005). *Perceived control: Scales for privacy in ubiquitous computing.* Rochester, NY: Social Science Research Network.

Spiekermann, S., & Berthold, O. (2004, December). *Maintaining privacy in RFID enabled environments—Proposal for a disable model.* Paper presented at the 2nd International Conference on Pervasive Computing, Vienna, Austria.

Spiekermann, S., Grossklags, J., & Berendt, B. (2001, October). *Stated privacy preferences versus actual behavior in EC environments: A reality check.* Paper presented at the Wirtschaftsinformatik [Business Informatics], Augsburg, Germany.

Spiekermann, S., & Ziekow, H. (2006). RFID: A systematic analysis of privacy threats and a 7-point plan to adress them. *Journal of Information System Security, 1*(3), 3-17.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science, 46*(2), 186-204.

Weiser, M. (1991). The computer for the 21st century. *Scientific American, 265*, 94-104.

Westin, A. F. (1991). *Harris-Equifax Consumer Privacy Survey 1991*. Atlanta, GA: Equifax.

Zhang, P., & Li, N. (2004, December). Love at first sight or sustained effect: The role of perceived affective quality on user's cognitive reactions to information technology. Paper presented at the Twenty-Fifth International Conference on Information Systems, Washington, DC.

Matthias Rothensee is a PhD student at the Institute of Engineering Psychology at Humboldt University, Berlin. Having received his diploma in 2005, he is working on social psychological influences on the acceptance of ambient intelligence technologies. He writes his PhD dissertation in cooperation with the Institute in Information Systems at Humboldt University Berlin. He can be contacted by e-mail at rothensee@wiwi.hu-berlin.de.

Sarah Spiekermann is assistant professor at the Institute of Information Systems at Humboldt University, Berlin, where she holds lectures for graduate students on the subject of "information systems and e-business" and regularly offers seminars on current topics in electronic markets. She can be contacted by e-mail at sspiek@wiwi.hu-berlin.de.