Sarah Spiekermann

User Privacy Concerns Surrounding the Introduction of RFID

Abstract RFID technology has received a lot of attention when it comes to technical proposals on how to maintain user privacy. Yet, few insights have been gained on what people really fear when they interact with the technology. Is it the flow of information between objects and unnoticed readers? Or do people fear the exchange of fine grained and individually attributable RFID data after collection? Is a psychology of ownership involved when readers access one's personal belongings? And do people oppose read-outs in any location? In order to win a better understanding of user concerns a series of focus groups was conducted. The qualitative results obtained show that people perceive a loss of control over information flows caused by RFID and that this loss of control is at the basis of concrete privacy breaches feared.

Keywords Privacy · RFID· User Control

1 Introduction

Reflections on potential privacy threats associated with RFID as well as technical proposals to safeguard the technology have been widely published in recent years (see for example: [1-4]. However, when starting out on the construction of privacy enhancing technical designs for RFID a thorough requirements analysis is recommendable [5]. The question is, whether privacy – although theoretically infringed upon by RFID technology – is really an issue for consumers to the degree that they will act upon its potential breach. For most E-Commerce environments information collection and secondary use seems to be accepted by consumers. Or, at least, privacy concerns echoed by consumers about online information collection practices are not mirrored in any protective actions or widespread use of privacy enhancing technologies [6-8].

Furthermore, privacy is a *"chameleon-like word"* [9]. Do privacy concerns in the context of RFID relate to 'information privacy' which could be sacrificed by any personally identifiable read-event? Or do peoples' concerns focus on highly personal objects the discovery of which could impact a person's dignity (for example, underwear). Do consumers desire for a general *"right to be let alone"* [10] or is their acceptance of surveillance through RFID readers linked to some territorial rationale [11]? [12] describes how privacy as a concept can be related to the right to be let alone, to limited access to the self, to secrecy, information control, personal dignity as well as intimacy. [13] frames privacy for Ubiquitous Computing referring to the aspects of solitude, confidentiality and autonomy. The question is what type of privacy do peple perceive as being breached when it comes to RFID? Neither the analysis of media messages nor prior scientific research shed light into this issue.

A content analysis of media-messages in 350 articles on RFID published in 68 national and international print and online outlets between May 2000 and April 2004 revealed that about 1/3 of print media messages and 40-50% of online media messages were related to consumer threats and that this critical media reporting tenor was on the rise in all media investigated [14]. More precisely, 71% of consumer fears reflected on in the German press in 2004 were related to the information collection and surveillance potential of RFID technology; referring either to governments (6%), to companies (39%) or to unauthorized third parties (26%). When criticism is voiced about RFID in the media themes raised are relatively unspecific to RFID technology though. They include terms such as "breach of privacy", "surveillance", "lack of transparency", "personal data" or "transparent customer". The highest degree of specificity vis-à-vis RFID is reached when articles report on potentially uncontrollable read-outs. Here, termini such as "without knowledge", "unnoticed", "calm and secret" are used. However, most of these descriptions could be equally applied to discuss the social challenges of many other information technologies. Content analysis of the general press therefore bears little potential to identify the concrete user concerns surrounding the introduction of RFID technology.

Sarah Spiekermann
Humboldt University Berlin, Germany
E-mail: sspiek@wiwi.hu-berlin.de

A first scientific study on RFID related consumer threats was conducted by GS1's adjunct technical unit, the Auto-ID Center [15]. 20 focus groups were organised in the US, Germany, Japan, France and the UK in order to better understand consumers' view of the technology. Here, the spontaneous reactions of consumers were investigated and potential negatives including effects of the technology for unemployment or health and for privacy were brought up. The result of this series of studies was that privacy issues are indeed at the top of peoples' minds and that, more precisely, the idea of being tracked, of other people knowing what one buys and personal security were at the forefront of consumer privacy concerns.

On the background of these insights and relatively sparse knowledge about consumer concerns surrounding RFID a more grounded qualitative research series was set up at the Institute of Information Systems at Humboldt University Berlin in 2004. The goal was to deepen the understanding of the concrete privacy concerns that people fear to be violated through the introduction of RFID.

2 Method

Three focus groups were conducted in a Berlin test studio. 8-9 Berlin citizens were recruited by a marketing agency. They were contacted via telephone and invited to join a two hour discussion on the future of shopping. Phone numbers were drawn from a random phone number generator, but the agency was briefed to provide a mix of sexes, age classes (between 20 and 60 years of age) and professional backgrounds.

The discussion was facilitated by a professional moderator and all spoken words were audiotaped and transcribed. Upon arrival, participants introduced themselves and a warm-up discussion was conducted on the benefits and drawbacks of loyalty cards. The reason for choosing loyalty cards as a starting subject was that it relates both to shopping and potential privacy issues. The moderator challenged the audience with a few privacy sensitive scenarios potentially arising in retail environments (such as the use of purchase data for unwanted secondary purposes). This biased start of the discussion allowed for preparing participants' critical consciousness before any mentioning of RFID technology. Then, an animated film was shown about the Metro Future Store and the future of shopping. The moderator informed participants that many of the new services shown to them would be based on RFID technology. Following a neutral script she explained the new retail services shown in the film such as personal shopping assistants on shopping trollies, smart shelves, individual advertisements, faster checkouts through RFID scans and also the RFID deactivator machine currently in use in the Metro Future Store in Rheinberg.

After this first film stimulus participants discussed the benefits and drawbacks of the services they had seen and now associated largely with RFID . Questions about the functioning of RFID and its potential as well as the possibility of deactivation were clarified. Then, a short documentary produced by one of Germany's main TV stations (ARD) was shown. This documentary commented on the potential privacy threats surrounding RFID.

3 Results

The goal of the focus group set-up was to understand user reactions to RFID upon full information about the technology's benefits and drawbacks. Explicitly, we did not leave participants in the dark about the technology's potentials, but wanted to observe the nuances in their reactions and the underlying reasons for fear of the technology. The main *issues* which were echoed by the 26 participants in the 6 hours of discussion can be summarized as follows:

3.1 Fear of losing control over information leaking about one's belongings

This is a primal fear of being out of control vis-à-vis the invisible and unnoticeable nature of a technology that can penetrate one's privacy boundaries and permeate and access information about one's belongings without one knowing whether and when this is happening. Loss of control is attributed to both, **not seeing the chip** (which may be embedded in the packaging): *"...but if I don't know where this thing is?*" or being **read out unnoticed over a distance**: *"...one does not know that someone accesses you, that is an awkward feeling"* or *"That was quite scary somehow, because one can be continuously observed... cameras can read the chips over a certain distance, so that one can get a real impression from a person when he carries these things [the chips]..."*

People seem to want to control the information that is being read out for distinct reasons: one is that the **information collected about them could be used against them**. This becomes apparent when people discuss the possibility that thieves could scan one's housing interiors (*"For sure it is such that a thieve could, if you are not there, hold the reader to the window...and read and scan your apartment from a 10 metres distance."*) or how they would prevent GEZ (the German body for collecting radio and TV fees) from reading out the presence of radios and TV stations (*"The GEZ...Then I buy a device...something that will send an interference signal so that one cannot see it [the TV/radio]"*). Another reason for this desire of not leaking information about one's belongings seems to reside in the **psychology of ownership** [16]. One group participant said: *"The product I have bought is my property and I want to do with it what I want. This is of nobody else's business."*

3.2 Information collection for personalization

A related threat echoed by the participants was that the automated and large-volume collection of object data could be used to accumulate knowledge about individuals. Here, concerns were less about one's individual objects being known to others or this awkward feeling of being scanned without knowledge, but the idea that one would **become known to others and transparent**: *"When someone collects information, then this also means accessing the person…"* or *"They know all about me and I know nothing about them".* They were afraid that based on this knowledge about them they would be confronted with personalized advertisements. However, this fear was not related to the individual treatment per-se. Instead it was reigned by their concern that their **weaknesses could be detected** by others and that they could be classified by retailers, for example, as 'low budget' and that a public display of personalized advertisements or messages could **reveal this classification to other**: *"…then they classify me as 'low budget' and then my neighbour stands next to me and says 'look' she is getting this cheap stuff again'…".*

3.3 Tracking of objects and people

Tracking of objects and people refers to the possibility that object information is being read out and used to create movement profiles. Individuals' whereabouts could be deducted by recognizing them via their objects. Among group participants this technical feasibility raised **fears of being chased** (*"I would start to constantly fear being tracked"*). Interesting enough though participants also seemed to **distinguish different territories** when they reflected on RFID tracking. In particular, they accredited retailers the right to track customers in their premises, but they insisted on their right that such tracking should stop at store exits: *"If chip services are only offered inside stores …then that's fine. But I would have a problem with further tracking outside stores"* or *"They can ue this in their environments, in their production facilities, in their sales rooms, but then that's it! Then they have to leave me alone. I leave the store and I do not want to be tracked."* This protectionist territorial thinking in judging retailers' rights to track individuals' outside of stores could be explained by humans' innate territorial behavior which attributes limited individual rights to publicly shared space [11, 17].

3.4 Abuse

On the background of these three threats to be read out unnoticed and from a distance, tracked and analysed by others participants generally felt uneasy about the possibility that RFID's technological capabilities could be abused by unauthorized parties generally. An **elusive impression of the potential abuse** of the technology to the detriment of others was echoed, but hardly specified: *"I also find this technology horrible and believe that it could quickly be abused in negative situations", "I think that it could quickly be abused in negative situations, such as for spying.*

3.5 Responsibility for objects

This fear relates to the potential association with and mapping of people to the objects they own or have owned in the past. Some of the fear is motivated by a potential **responsibility for the misuse or fate of objects.** An example is the discovery of a wrong disposal of an object by its owner and the potential traceability of such behavior by others: "*Yes, I know these janitors who search the garbage to see whether someone has sorted something wrong into it. That is a really stupid thing. [if that was the case with RFID] I would never buy something with a card [electronically] any more."* The **sheer volume of objects one possesses** and for which such responsibility could be established is another source of peoples' concern: *"Then I am responsible as a buyer for the yoghurt can or what? That's crazy!"* Consequently, participants strongly opposed the idea to have a potential link created between themselves and the objects they own: *"…but what is important to me is that I am not linked as a person to the product that I have bought".*

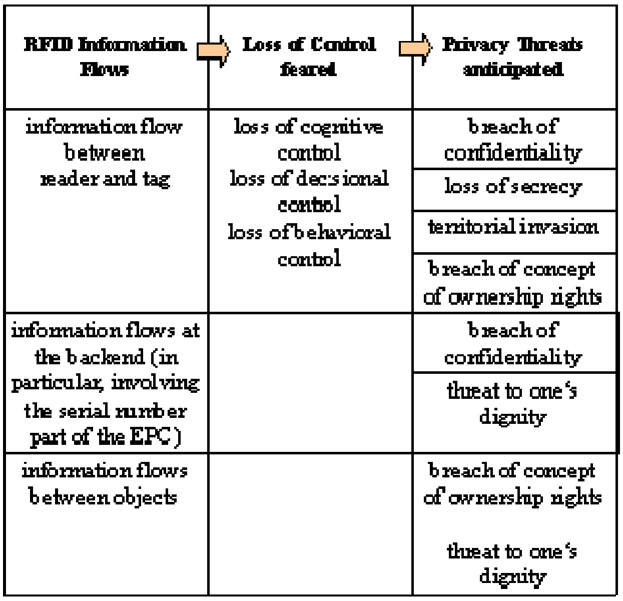
3.6 Technology Paternalism

This fear relates to the possibility that RFID technology could be used to 'paternalistically' regulate peoples' behavior by observing and influencing their interactions with objects [18, 19]. RFID inherently bears the characteristic of object-object recognition. It can thus detect whether products, objects, infrastructures and components fit together. For example, it could be used to detect whether a battery is allowed in a paper garbage can. Or it could enforce the use of complementary products from a single manufacturer. Focus group participants echoed this negative aspect of the technology with a view of being potentially **embarrassed** (*"The question is whether it starts beeping when I leave the yoghurt besides the cashier, and then there is a signal, and then everybody knows…"*) or **being restricted** by their objects to act in a certain way: *"I imagine myself taking a nice caviar box and then my computer tells me 'no, this is not for you'."*

4 Discussion

At their very origin all privacy threats mentioned by the participants could be interpreted as originating from a loss of control over information flows. Information flows between individuals' objects and the reader infrastructure, information flow between objects, and information flows happening at the collecting unit's network backend. Some participants verbalized this loss of control *"…something is being done with me which I cannot really control and review and this is threatening me", "Who is supposed to control all of this? That the data is not finally used for other purposes?"* Table 1 visualizes the sequential relationship between information flows caused by RFID, the subsequent loss of control (if no PETs are available) and the resulting perceived threat to privacy. The sequence is inversely based on [11] who defines privacy as *"control over access to the self"*. As the information flows caused by RFID abscond from user control, access to the self (privacy) is perceived as not manageable any more.

Table 1 Relationship RFID, Control and Privacy



RFID Information Flows	Loss of Control feared	Privacy Threats anticipated
information flow between reader and tag	loss of cognitive control loss of decisional control loss of behavioral control	breach of confidentiality
		loss of secrecy
		territorial invasion
		breach of concept of ownership rights
information flows at the backend (in particular, involving the serial number part of the EPC)		breach of confidentiality
		threat to one's dignity
information flows between objects		breach of concept of ownership rights threat to one's dignity

According to [20] on could argue that RFID systematically deprives people of all three forms of control distinguished by behavioural psychology: 1. cognitive control, which is a person's possibility to understand and interpret threatening events, 2. behavioural control, which is the possibility to take direct action on the environment in order to influence threatening event and 3. decisional control, which is the opportunity to choose among various possible actions. The fact that people may not necessarily know about the presence of an RFID chip, may not be aware of distanced readers and cannot see communication taking place undermines their cognitive control over RFID. The flow of information between their objects (them) and the reader infrastructure is not apparent to them. But even if communication was made visible to them no technological means are embedded in the RFID infrastructure as of today to give people the possibility or choice (behavioural and decisional control) to prevent this flow of information from happening. As a result of this lack of control people express the fear of a loss of confidentiality or even breach of secrecy. People want to maintain control over outgoing information flows in order to conceal information about themselves that others might use to their disadvantage once they know about their belongings. Moreover, they feel that they have the right to control the information leaving the objects they possess; a concept explicable by the psychology of ownership [16]. Use of RFID information against them is not only an incident feared with a view to RFID readouts of objects, but also with a view to the flows of RFID based information at the backend. Even if consumers were notified and informed about the further processing of RFID event data, the question is to what extend this information will be complete and comprehensive enough to provide sufficient cognitive control over what is happening. A feeling of decisional control may be induced in consumers if they are given a choice to 'opt out' of RFID data processing. But still no behavioural control can really be exercised to control data flows at the backend. As a result, consumers cannot know for sure whether some attribution between them and the individual products they purchase is finally being made. The EPC's potential to create one-to-one links between objects and people at the backend could thus represent another kind of breach of confidentiality: People fear to be classified and profiled and by such practices be potentially identified as having weaknesses. Equally, they seem to fear that interactions with objects they own could be critically observed or at least recapitulated. For example, whether they have thrown objects away, have broken them or misused them. The detection of such misbehaviour would again represent a breach of confidentiality.

Peoples' desire to control the objects they own is also closely related to the concept of autonomy. Autonomy is defined as the freedom to set one's own goals and to have the freedom to pursue them in the way one desires [21]. If objects are designed to communicate with each other the flow of information between objects could be as intransparent to users as is the case for object-network communication depriving them of cognitive control. Then, they may be impacted in their autonomy to use objects in the way they want to (technology paternalism). For example, the user of a drilling machine may be impeded to use it if he does not wear proper protection glasses from the same manufacturer. Equally, the wrong placement or non-placement of objects could lead to embarrassing signals. A current non-RFID example of such machine reactions are beeping signals in cars when drivers forget to put on their seatbelts. Object-to-object information flow which triggers some type of machine reaction therefore has the potential to intrude upon peoples' privacy if they happen to be detected in and exposed for false behavior. [12] would refer to this type of privacy breach as an assault on dignity or personhood.

Finally, the focus groups revealed one further aspect of privacy in the context of RFID which is the one of territoriality. People seem to accept RFID readouts done by retailers in their 'primary territories' in the stores, but not so in shared territory (outside stores). In accordance with [11] it could therefore be speculated that the desire to control the flow of RFID information and thus actively manage privacy is depending on the territorial context of the individual.

References

1. Sarma, S., S. Weis, and D. Engels, *RFID Systems, Security & Privacy Implications*, A.-I. Center, Editor. 2002, Massachusetts Institute of Technology, MIT: Cambridge, USA.
2. Juels, A., *RFID Security and Privacy: A Research Survey.* IEEE Journal on Selected Areas in Communication, 2006. **24**(2): p. 381-394.
3. Langheinrich, M., *Die Privatsphäre im Ubiquitous Computing - Datenschutzaspekte der RFID-Technologie*. 2004, ETH Zürich: Zürich.
4. Spiekermann, S. and O. Berthold, *Maintaining privacy in RFID enabled environments - Proposal for a disable-model*, in *Privacy, Security and Trust within the Context of Pervasive Computing*, P. Robinson, H. Vogt, and W. Wagealla, Editors. 2004, Springer Verlag: Vienna, Austria.
5. Hoffer, J.A., J.F. George, and J.S. Valacich, *Modern Systems Analysis and Design*. 2002, New Jersey: Prentice Hall.
6. Berendt, B., O. Guenther, and S. Spiekermann, *Privacy in E-Commerce: Stated Preferences vs. Actual Behavior.* Communications of the ACM, 2005. **48**(4).
7. Acquisti, A. and J. Grossklags, *Privacy and Rationality in Individual Decision Making*, in *IEEE Security & Privacy*. 2005. p. 24-30.
8. Spiekermann, S., J. Grossklags, and B. Berendt. *E-privacy in 2nd generation E-Commerce*. in *Proceedings of the 3rd ACM Conference on Electronic Commerce EC'01*. 2001. Tampa, Florida, USA: ACM Press.
9. Solove, D.J., *A Taxonomy of Privacy.* University of Pennsylvania Law Review, 2005. **154**.
10. Warren, D. and L. Brandeis, *The Right to Privacy.* Harvard Law Review, 1890. **4**(5).
11. Altman, I., *The environment and social behavior: Privacy, personal space, territory, crowding*. 1975, Monterey, California: Brooks/Cole.
12. Solove, D.J., *Conceptualizing Privacy.* California Law Review, 2002. **90**: p. 1087-1156.
13. Boyle, M. *A Shared Vocabulary for Privacy*. in *Fifth International Conference on Ubiquitous Computing*. 2003. Seattle, Washington.
14. Falter, M., et al., *Die Wahrnehmung von RFID in den Medien – Eine Inhaltsanalyse*, in *Arbeitsbericht*. 2004, Humboldt-Universität zu Berlin, Institut für Wirtschaftsinformatik: Berlin.
15. Duce, H., *Public Policy: Understanding Public Opinion*, A.-I. Center, Editor. 2003, Massachusetts Institute of Technology, MIT: Cambridge, USA.
16. Pierce, J.L., T. Kostova, and K.T. Dirks, *The State of Psychological Ownership: Integrating and Extending a Century of Research.* Review of General Psychology, 2003. **7**(1): p. 84-107.
17. Lyman, L.M. and M.B. Scott, *Territoriality: A neglected sociological dimension.* Social Problems, 1967. **15**(2): p. 235-249.
18. Spiekermann, S. and F. Pallas, *Technologiepaternalismus – Soziale Auswirkungen des Ubiquitous Computing jenseits von Privatsphäre*, in *Die Informatisierung des Alltags. Leben in smarten Umgebungen.*, F. Mattern, Editor. 2007, Springer: Berlin Heidelberg New York.
19. Spiekermann, S. and F. Pallas, *Technology Paternalism - Wider Implications of RFID and Sensor Networks.* Poiesis & Praxis - International Journal of Ethics of Science and Technology Assessment, 2005. **4**.
20. Averill, J.R., *Personal control over aversive stimuli and its relationship to stress.* Psychological Bulletin, 1973. **80**: p. 286-303.
21. Volpert, W., *Handlungsregulation*, in *Handbuch Arbeitswissenschaft*, H.v. Luczak and W. Volpert, Editors. 1997, Schäffer-Poeschel: Stuttgart. p. 453-458.