By Oliver Günther and Sarah Spiekermann

Consumers need to feel they have control over the RFID infrastructure before they routinely trust its services.

RFID and the Perception of Control: The Consumer's View

In his seminal 1991 *Scientific American* article "The Computer for the 21st Century," Mark Weiser, an early visionary of ubiquitous computing, wrote "the [social] problem [associated with ubiquitous computing], while often couched in terms of privacy, is really one of control." The ongoing public debate over RFID technology and how it might affect consumer data privacy in the retail industry very much reflects this tension between control and privacy.

The Metro Group Future Store Initiative represents the first large-scale rollout of RFID technology in a retail context (www.future-store.org). We have been working for the past year with Metro Group to identify consumers' major privacy fears relating to RFID and develop and evaluate appropriate privacy-enhancing technologies (PETs). Here, we analyze the results of our empirical study of ordinary German retail consumers conducted in the spring of 2005. We gave a representative sample of 129 consumers two distinctly different types of PETs, one user-based, one agent-based. Their reactions reflected considerable distrust of RFID-based environments; for example, 73% preferred RFID

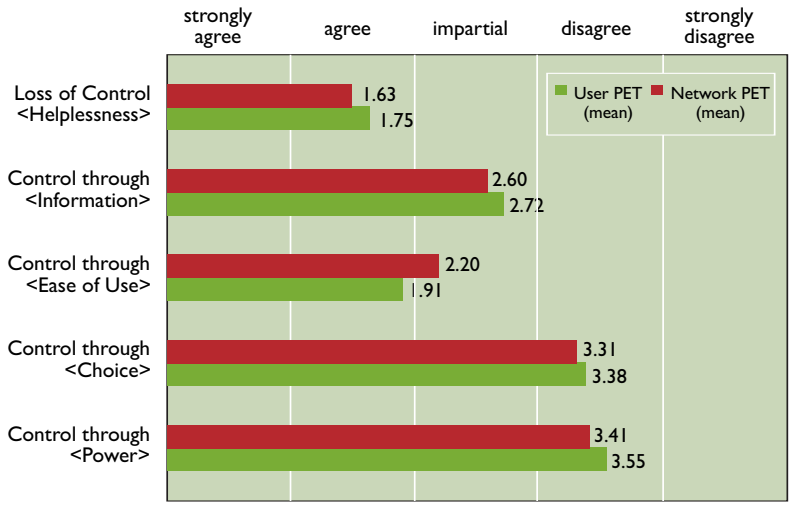

Figure 1. Mean perception of control for two types of privacy-enhancing technology.

deactivated permanently at checkout time, regardless of potential consumer benefits (such as claiming warranties without a receipt) and of the PETs we offered them. For highly educated consumers, this percentage was 78%. Retailers worldwide must address these concerns if RFID is to succeed.

Perception of Lost Privacy

In ubiquitous computing (UC) environments, including future RFID-enabled shopping malls, the perception of lost privacy seems to be due to two factors:

Being accessed. Some researchers refer to this privacy aspect of these environments as the need to control the *attention* of the environment. Focus groups at AutoID-Labs (an industry-sponsored RFID research network of seven laboratories worldwide) and at Humboldt-Universität Berlin have shown that ordinary consumers are particularly apprehensive about RFID technology. The risk is it may allow third parties to determine personal behavior and track individuals' physical movements without prior notice.

Information dissemination, use, and maintenance. RFID has added a new dimension to the traditional e-privacy debate, because much more data can potentially be collected about individuals. Potential tracking of personal whereabouts and social network analysis has gained a "physical" dimension. Unique item identification inherent in the proposed Electronic Product Code (EPC) standard can potentially lead to a degree of personal attribution and surveillance never before possible.

Secondary use (and abuse) of information is not possible if access is prohibited in the first place. That is why controlling access is a critical factor in the RFID privacy equation. Not surprisingly, access control is being investigated in a number of research efforts, especially those focusing on privacy-preserving identity management systems. In our study with Metro Group, we investigated whether ordinary consumers would feel they had control over RFID-enabled intelligent infrastructures if they were given a PET to guarantee their privacy was being shielded. The two PETs we tested differ in one key way: whether control is exercised directly by the individual (user model) or delegated to an agent (agent model):

User model. The user model implies that users exert full control over RFID tags by means of appropriate authentication mechanisms. Objects do not by default respond to network requests. Instead, the user self-initiates intelligent services, if available and useful in the respective context. The context decisions concerning when and how the use of tags is appropriate is thus taken by the object owner [3]. If the owners of

Regardless of privacy-enhancing technology employed, consumers feel helpless toward the RFID environment, viewing the network as ultimately more powerful than they can ever be.

objects gain some benefit from activating the object's RFID tag they can do so by authenticating access, typically through a password.

Agent model. In contrast, the agent model is based on the idea that RFID tags are active by default, constantly responding to network requests. Access control in this scenario is delegated to an agent, typically a privacy-preserving identity-management system storing consumer privacy preferences. Based on the predefined preferences, the system takes the context decision autonomously and decides when to answer network requests, when to deny them, and when to ignore them [1].

Do these protection mechanisms increase consumer acceptance of RFID? Which one of the two models gives retail consumers a greater degree of perceived control? And, consequently, which gives a greater degree of perceived privacy?

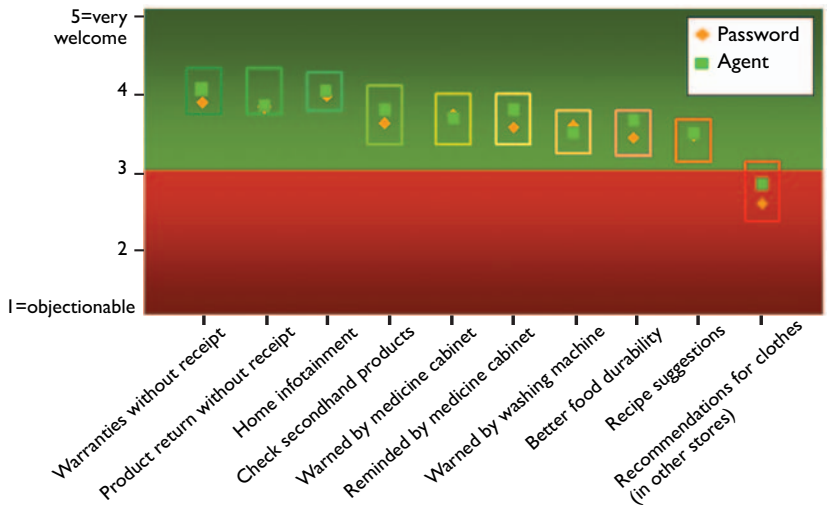

Figure 2. Appraisals of potential RFID after-sales consumer benefits.

Empirical Study

Our study involved 129 subjects demographically representative of the overall German population: 47% were female; 53% were male; 36% were younger than 30 years of age; 21% were between 30 and 39; and 43% were 40 years or older. Reflecting educational background, 25% held a university degree; 35% had graduated from high school but had not completed university education; and 40% left school with an intermediate or no degree before the age of 18. We split participants into two groups, one with 74 subjects, the other with 55 subjects. Each group was shown a film on future shopping environments in which RFID technology would be used. We explained RFID technology neutrally and its benefits and drawbacks without bias. We described after-sales benefits of RFID on the basis of two services: an intelligent refrigerator and product return without need of a receipt.

The film we showed was the same for both groups except for the PET available to consumers for controlling their privacy. In Group 1 (user model) the film explained that RFID tags would all be protected at checkout time using a personal password. This temporary deactivation would occur automatically without incurring any delay or complications at checkout. We told participants that they could reactivate tags by using their PINs in case they would want to use some after-sales service.

In Group 2 (agent model) the film explained that tags would all be left on at checkout time but could be accessed only by RFID readers for after-sales purposes if the network's stated purpose matched the consumer's privacy preferences. These preferences would be stored on the network, in our case with a mobile phone operator serving as a "privacy buffer." If a reader's request did not match the given privacy preferences, access to the tags would be blocked.

Before and after they saw the film, participants answered a number of questions. We developed a 10-item scale in advance of the film, based on a separate study of appropriate measures for perceived control [2]. We defined perceived control as the belief people have in the electronic environment acting only in ways that were explicitly allowed. Factor analysis of the control items revealed that perceived control over RFID can be measured in negative terms by asking consumers about the degree of helplessness they perceive vis-à-vis the intelligent infrastructure. They can also be asked about the degree to which they feel informed about what is happening and their competence handling their RFID-related communication. Figure 1 is an overview of the perceived control measured. Regardless of PET employed, consumers feel helpless toward the RFID environment, viewing the network as ultimately more powerful than they can ever be.

This sense of powerlessness is also reflected in the negative perception they have of their options. Ordinary consumers do not think the intelligent infrastructure will leave them alternatives or obey their privacy preferences. They are also not sure whether

Better-educated consumers feel even less informed, less empowered, less able to make choices, and more helpless in the face of ubiquitous RFID technology than those without higher formal education.

sufficient information will be available to them to exercise control over being surveilled through the network. This negative overall perception dominates despite the fact that these consumers considered both PETs fairly easy to use; neither PET was a clear favorite from the user perspective.

These results were further reflected in answers given at the end of the questionnaire where we asked the subjects to render a final judgment as to whether they prefer being protected by the respective PET or having RFID tags killed at checkout time. Even though they had been through a long list of questions concerning potential benefits of RFID and despite the fact that they rated most of these benefits as interesting and positive (see Figure 2), 73.4% of the subjects reported preferring to have the RFID tags killed at checkout time. Meanwhile, only 18.0% were willing to trust the PET, and 8.6% were undecided. Comparing the two PET types, the agent model (78.2% rejection) prompted even more skepticism than the user model (69.9% rejection), though the difference was not significant.

Since RFID technology and its consumer implications may be difficult to grasp, we also analyzed a subsample, including 60% of the subjects with at least high school educations. Their negative perceptions concerning control increased for all items. In other words, better-educated consumers feel even less informed, less empowered, less able to make choices, and more helpless in the face of ubiquitous RFID technology than those without higher formal education. For the user-based password scenario, this trend is statistically significant for almost all measures of control. As for the agent model, the better-educated subjects still preferred permanent deactivation, though this trend was not significant and represented a notable difference from the general sample. A more advanced technical understanding by the people in the subsample probably made it easier for them to appreciate the advantages of the agent model.

Conclusion

Our recent study of German consumers found they feared losing privacy due to the introduction of RFID technology. Even though the potential advantages of RFID (such as enhanced after-sales services) are well understood by a solid majority of consumers, fear seems to override most of these positive sentiments. Retailers must address this fear if they are to have any hope of making RFID a widely used business tool that gives consumers greater convenience in the long term. An open dialogue about the technology's advantages and potential dangers is an important step in this direction. C

References

1. Floerkemeier, C., Schneider, R., and Langheinrich, M. Scanning with a purpose: Supporting the fair information principles in RFID protocols. In *Proceedings of the Second International Symposium on Ubiquitous Computing Systems* (Tokyo, 2004).
2. Spiekermann, S. Perceived control: Scales for privacy in ubiquitous computing environments. In *Proceedings of the 10th International Conference on User Modeling* (Edinburgh, Scotland, 2005).
3. Spiekermann, S. and Berthold, O. 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, Eds. Springer Verlag, Vienna, Austria, 2004.

Oliver Günther (guenther@wiwi.hu-berlin.de) is the director of the Institute of Information Systems at Humboldt-Universität zu Berlin, Berlin, Germany.
Sarah Spiekermann (sspiek@wiwi.hu-berlin.de) is an assistant professor in the Institute of Information Systems at Humboldt-Universität zu Berlin, Berlin, Germany.