Privacy Enhancing Technologies for RFID in Retail-An Empirical Investigation

Sarah Spiekermann

Institute of Information Systems, Humboldt University Berlin,
Spandauer Strasse 1, 10178 Berlin, Germany
sspiek@wiwi.hu-berlin.de

Abstract. This article investigates the conflicting area of user benefits arising through item level RFID tagging and a desire for privacy. It distinguishes between three approaches feasible to address consumer privacy concerns. One is to kill RFID tags at store exits. The second is to lock tags and have user unlock them if they want to initiate reader communication (user scheme). The third is to let the network access users' RFID tags while adhering to a privacy protocol (agent scheme). The perception and reactions of future users to these three privacy enhancing technologies (PETs) are compared in the present article and an attempt is made to understand the reasoning behind their preferences. The main conclusion is that users don't trust complex PETs as they are envisioned today. Instead they prefer to kill RFID chips at store exits even if they appreciate after sales services. Enhancing trust through security and privacy 'visibility' as well as PET simplicity may be the road to take for PET engineers in UbiComp.

Keywords: RFID, privacy, security, privacy enhancing technology, RFID kill-function, authentication, identification, user behavior.

1 Introduction

Radio Frequency Identification (short RFID) is considered to be an important technological building block of Ubiquitous Computing. Provided that RFID tags are embedded in everyday objects and accessed by a networked reader infrastructure, it will be possible to create myriad new information, tracking and access services across industries. A relatively new and promising application domain for RFID is the retail sector. Retailer logistics, shop-floor management, marketing and after-sales services are all in the verge of being optimized with the help of RFID. As a result, retailers and their product suppliers are now starting to deploy RFID tags as the next generation bar code on individual products.

However, the introduction of RFID on products has met criticism in the press and through privacy rights organisations to an extent that – despite all expected benefits – retailers hesitate about whether and how to fully launch the technology in areas where it interfaces with consumers [1]. On the shopfloor, recognizing customers individually and automatically upon arrival, tracking them through the store, observing their interactions with products and offering them personalized advertisements and

J. Krumm et al. (Eds.): UbiComp 2007, LNCS 4717, pp. 56–72, 2007.

information services are all activities which can be realized through RFID, but have the potential to be viewed as privacy intrusive [2-4]. More important, privacy advocates point to retailers' responsibility to not let RFID enabled products leave their stores. They fear that accessible RFID tags on most objects in the public domain will lead to ubiquitous surveillance of people [5]. And indeed, their concerns are reflected in qualitative research studies with consumers on the technology. In 2004 four focus groups were organized in Berlin with 30 participants discussing RFID in a retail context. They were shown 2 films (a positive and a critical one) about the technology to inform about RFID, its service vision, benefits and potential ethical drawbacks. Focus group participants were recruited by a research agency to represent a spectrum of consumers similar to the German population in terms of age, sex and education. Based on these recorded sessions and transcribed discussions six major privacy concerns could be discerned (free translation of citations) [4]:

(1) **Fear of losing control over one's belongings:** "…but if I don't know where this thing is?", "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."
(2) **Tracking of objects and people:** "If chip services are only offered inside stores …then that's fine. But I would have a problem with further tracking outside stores", "I would start to constantly fear being tracked."
(3) **Responsibility for objects** (due to the individual attribution of unique products to people): "…but what is important to me is that I am not linked as a person to the product that I have bought", "Then I am as a buyer responsible for the yoghurt can? That's crazy!"
(4) **Technology paternalism** – the idea that objects recognize and punish misbehaviour: "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…", "I imagine myself taking a nice caviar box and then my computer tells me 'no, this is not for you'."
(5) **Information collection and personalization** (due to recognizing individual product IDs): "…then they classify me as 'low budget' and then my neighbour sees that I am only offered the cheap stuff", "They know all about me and I know nothing about them."
(6) **Abuse** (attacks on one's privacy by hackers or other unauthorized parties): "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."

One major conclusion drawn by the observers of the focus groups was that participants seemed to unanimously call for RFID tags to be killed at retailer exits. Emotional levels seemed to rise considerably when people learned that they would carry multiple functioning chips with them out of the store. And it seemed as if they were drawing a line of legitimacy for RFID use by retailers in their own proper facilities, but not beyond: "They can use this technology in their business environment, their production units, their sales domain, but that's it! Then they have to leave me alone. I leave the store and I don't want to be tracked". Results equally critical of RFID technology were also obtained in focus groups conducted by the Auto-ID centre in the US, UK, France and Japan [6].

Given these qualitative research results, a question confronted by retailers today is how to treat RFID chips at store exits. Should they make use of the kill-function foreseen in the generation 2 specification for mass-market class 1 RFID chips [7] and permanently deactivate tags' functionality to transmit data when their buyers leave the store? Or should they ignore consumer and privacy rights calls and leave the chips' functionality intact? Might it be a viable option for them to demand the inclusion of privacy enhancing technologies (PETs) in the RFID infrastructure so that RFID tags are not killed at store exits, but only accessible by authorized entities? And if so, which PETs should retailers support? To answer these questions, retailers need to understand how vital the privacy issue really is for their customers and how willing they are to trade their concerns with the technology's benefits; in particular, in the after-sales domain where permanent deactivation of RFID tags would impede any further service potential.

Against the background of these questions two quantitative consumer studies were conducted in co-operation with the Metro Group from 2004 to 2006. The Metro Group is Europe's largest retail company. The goal was to assess peoples' perception of different technological scenarios to treat RFID at store exits and to understand the role of peoples' RFID usefulness perceptions in this conflicting area. Furthermore, individual attitudes towards privacy, group pressure and general technical affinity were included as independent variables to potentially explain preferences for different exit solutions. In the following sections, this paper will present the hypotheses and technological proposals which have driven this research effort (section 2), the experimental set-up used (section 3) and results obtained (section 4). In a final section implications will be deducted for those who build and deploy RFID to create intelligent infrastructures (section 5).

2 Privacy Enhancing Technologies for RFID and User Perceptions

RFID technology comes in many different forms. Tag classes ranging from 0 to 4 can be discerned depending on the tags' memory, power source and features [8]. Furthermore, tags operate at different frequencies and as a result employ very different transmission mechanisms with distinct read-ranges, bandwidths and capabilities to penetrate line-of-sight barriers. Much of the technology to date has been built to serve the needs of closed proprietary systems with specific use cases. Depending on the RFID system chosen for a specific purpose privacy problems can more or less arise. For example, RFID chips which transmit data over an UHF band (typically at 865 – 928 MHz) currently have reliable read ranges of around six to eight meters. In contrast, tags which transmit their data at 13,56 MHz only achieve reliable read ranges of around 1 ½ metres. As this comparison makes plain, privacy implications of RFID technology vary: the probability that an attacker can read out a person's belongings unnoticed is much more likely in an UHF scenario than it is in a 13,56 MHz environment. For this reason, the research presented hereafter needed to be grounded in a specific type of RFID deployment scenario. More precisely, the author built her research on the assumption that EPCglobal's class 1 generation 2

RFID tags and infrastructure vision would be deployed on an item level [7, 9, 10]. EPCglobal is today's main private international standardization body for both future numbering standards as well as the technical infrastructure for number processing (based on RFID). The organisation envisions all items to carry a passive UHF tag with one unique identifier, the electronic product code (EPC) [11]. The EPC is supposed to be used as a key to find information about the item it is attached to. This information is maintained within a backend network consisting of myriad EPC-Information Services (EPC-IS) [12]. These services can be accessed via an Object Name Service (ONS) and are ubiquitously accessible provided that the retriever holds respective access rights [13].

2.1 PETs for RFID – A Classification for Empirical Investigation

From a bird's eye three major blocks of PETs for RFID can be discerned for the after-sales area. First, the most straight forward approach is to simply kill the tags' ability to transmit its electronic product code (EPC). This solution is embedded in EPCglobal's generation 2 specification for mass market class 1 tags [7]. It would entail retailers to integrate a kill-command into their electronic check-out processes. From a technological standpoint it is the most radical privacy solution, but from a market perspective it implies the disadvantage that after sales scenarios for using RFID would equally be killed.

A second set of PETs builds on the vision that users exert immediate control over their RFID tags at the client side. These solutions are proposing that tags are 'locked' before leaving stores, but can be unlocked with the help of user controlled authentication mechanisms. As a result, object tags do not a priori respond to network requests. Instead the user self-initiates the use of intelligent services if they are available and useful in the respective context. The context decision when and how the use of tags is appropriate in a situation is thus taken by the object owner [4, 14-17]. If the owner of an object has some benefit from reviving an object's RFID tag and transmitting its information she can do so by authenticating herself vis-à-vis the tag and then give the tag explicit and situation specific permission to release its data. The authentication process would typically be handled via a password scheme where one or multiple passwords are either remembered by users or stored in a separate mediating device which maintains some type of password management system. However, regardless of the concrete authentication process and mechanism chosen (i.e. with separate user device or without separate user device; via passwords or via biometrics) the architectural vision puts the user in the role of the *initiator* of communication with the intelligent infrastructure. Hereafter, we want to refer to PETs in this domain as "User PETs". An underlying hypothesis to the current work was that User PETs should lead to a high level of perceived control with users since the intelligent infrastructure does not act in a pro-active manner. Figure 1a illustrates this interaction paradigm by visualizing it as a password protection scheme.

In contrast to User PETs, "Agent PETs" are based on the idea that RFID tags are unlocked by default and that the network takes the initiative to communicate with a user's tags. Access control to user tags in this scenario is provided (automatically) via some "watchdog" device carried by the user (i.e. a PDA) [18-20]. This device may - in the long run - determine whether the reader infrastructure has the right to access a person's tag(s) by transferring "mother" rights to a network once the network reader has proven its identity and adherence to a user's privacy preferences [21]. It could run a protocol similar to the one specified by the Platform for Privacy Preferences Project (P3P) in the context of E-Commerce transactions. P3P enables websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents [22]. Metadata included in this protocol comprise, for example, the type of information collected, the purpose of information collection and URIs to the data collector(s). In the RFID context first efforts have been made to integrate this metadata information into the generation 2 reader - tag exchange protocol [18, 20]. So far, however, watchdog devices are only able to display that communication has happened. In the context of the empirical studies presented hereafter it has been assumed that network requests to access RFID chips would be negotiated by a user's device. Figure 1b illustrates this interaction paradigm visualizing a mobile phone as the network interface and shield to users' RFID tags.

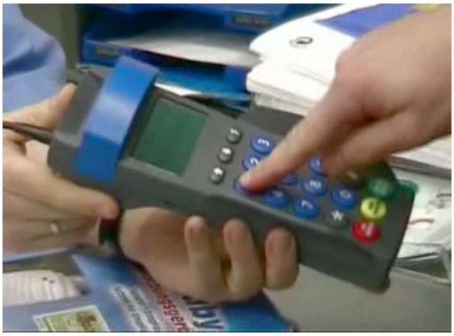

Fig. 1a. The User Scheme: Users personally initiate the communication of their tags and take the context decision to start exchange

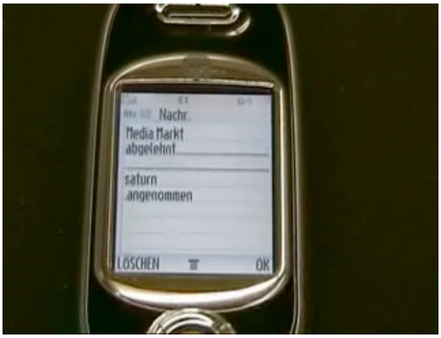

Fig. 2b. The Agent Scheme: Users delegates tag – network communication to phone agent and network takes context decision to start exchange

Of course, it must be acknowledged that more PET technologies are in the verge of creation or have already been proposed such as blocker tags [23] or mechanisms to physically destroy tag antennas [24]. Not all of these technologies may strictly adhere to one of the two paradigms of interaction. However, the author of this paper does believe that also in the long run one key question is whether a user initiates a data exchange selectively and upon taking the context decision to interact or whether the network will take care of this decision pro-actively. In the following sections the two distinct interaction paradigms are being compared empirically and it is being investigated how they are perceived by users relative to the most radical PET solution which is to kill RFID tags altogether. We will refer to the User and Agent scheme as "complex PETs" as opposed to the kill approach.

2.2 Hypotheses

Qualitative user studies and media attention to RFID drive retailers to seriously consider PETs at store exits. But which of the three schemes should they prefer? An important factor for answering this question is the degree to which buyers will want to take advantage of after-sales services available through RFID. It seems rational to expect that consumers who appreciate after-sales RFID services would prefer to know that threats to their privacy are being avoided while valued services are still available to them. We therefore hypothesize that for those consumers who appreciate after sales RFID services any PET scheme, whether that be the user scheme or the agent scheme is superior to chips being killed:

H1: The user scheme is considered superior to the kill option if people appreciate after-sales RFID services.

H2: The agent scheme is considered superior to the kill option if people appreciate after sales RFID services.

As was argued above, users are in the driver's seat if they initiate the communication between their tags and the network. It therefore seems sensible to expect that users will perceive more control over their RFID tags' communication when being confronted with a User Scheme than when delegating privacy decisions to an agent. And they will rather want to kill tags in an agent scheme scenario than in a user scheme scenario. We therefore hypothesize:

H3: When confronted with an Agent PET users will want to kill RFID tags more readily than when confronted with a User PET.

H4: The User PET is perceived by users to provide more control to them over the reader infrastructure than the Agent PET.

Finally, retailers need to understand the dynamics behind buyers' appreciation of more complex PETs versus the killing of tags. What would drive buyers to rather kill a tag or use a complex PET? An immediate answer could be that the ease of use of a complex PET drives this decision. But equally, the degree to which one feels informed as well as (intuitively) protected through the PET is important. These three factors, ease-of-use of the PET, information and reduction of helplessness through the PET (vis-à-vis an intelligent infrastructure) have been identified in earlier work of the author as constructs to measure the perceived effectiveness of PETs [25]. They were therefore included in the current work as independent dimensions driving the judgement of complex PETs.

In addition to this control perception of complex PETs, the theory of reasoned action [26] suggests that other attitude elements as well as peer opinions (subjective norm) play a role when humans determine their intentions to act (or use a technology). In the current context, theory of reasoned action was used as an underlying framework to identify constructs potentially influencing the use of complex PETs. For example, it could be argued that the perception of RFID services as useful will drive peoples' intention to adopt complex RFID PETs, because only these PETS will allow for maintaining the technology's valued services. Equally, ease of use anticipated for the technology could play a role for attitude formation. Finally, the influence of valued peers may be important [27, 28]. If RFID services are going to be appreciated by one's peer group, the likelihood to equally embrace the technology's service spectrum and not kill it will probably increase. Against this background the following hypothesis was formulated:

H5: A common set of technology acceptance factors, namely the perceived usefulness and ease of use of RFID, perceived control through the PET and the opinion of others on RFID will drive users' preference to prefer complex PETs for RFID over a kill approach.

Personal factors may equally play a role in how people judge PETs. Innovation diffusion theory has found that peoples' openness towards new technologies and technical affinity are an important characteristic of 'innovators' who are typically the first ones to try a new technology [29]. If people have these characteristics they may want to take advantage of RFID after sales services. Furthermore, they may be less afraid to embrace more complex PETs.

Finally, compatibility of a new technology with existing social and ethical standards as well as practices is important for adoption [29]. Therefore, the personal awareness for one's privacy maintenance could play a role for PET choice: If people are highly privacy sensitive they may have a tendency to prefer the more radical solution to kill RFID chips rather than to use a complex PET. Based on this reasoning we formulated hypothesis 6:

H6: Personal characteristics, in particular technical affinity, privacy attitudes and general attitudes towards new technologies have an impact on the preference for complex PETs over killing chips.

3 Method

3.1 Participants and Procedure

Two empirical studies were conducted following the same experimental procedure. 234 participants were recruited for study ① by a market research agency in the city of Berlin. They were selected to reflect average German demographics in terms of age, sex, education and income. One year later, the same study was replicated with an extended questionnaire including 306 participants. Participants for this study were recruited according to the same demographic parameters but included urban citizens from four different German regions.

Participants were briefed to participate in a study conducted by Humboldt University on the future of shopping and invited to a hotel in the respective region. Upon arrival, they received an initial questionnaire addressing their satisfaction with current retail environments and investigating their current knowledge about RFID (both studies). Study ② additionally included the measurement of attitude towards new technologies, technical affinity and privacy attitudes. Participants then watched a film informing them about RFID technology and future services on the shopfloor and after sales. Before seeing the film 86% had never heard about RFID in study ① and 81% in study ②.

Table 1. Experimental groups and demographics

		Study ①				Study ②	
		Chips ON	Chips Killed	User PET	Agent PET	Chips ON	User PET
Stimulus used		Film 1	Film 2	Film 3	Film 4	Film 1	Film 3
Film evaluation						6,9/11	7,7/11
Sex	Male	26	28	34	27	47	103
	Female	27	23	40	28	50	104
Age	< = 29	21	15	28	19	35	67
	30-49	23	26	34	26	56	134
	> = 50	9	10	12	10	6	6
Education	No high-school	25	21	31	20	42	81
	High-school	28	29	41	35	55	122
Income pre tax	< € 10 k	21	20	26	24	33	66
	€ 10 - 30 k	22	15	33	17	25	62
	> € 30 k	8	14	10	14	29	64
TOTAL		54	51	74	55	98	208
		234				306	

The film material used in these two quantitative studies was a different material than the ready-made RFID documentations used in earlier focus groups. It was exclusively produced to inform people in a neutral manner about RFID services as well as different potential PET solutions envisioned by engineers. The four different PET options (kill, chips left on, user or agent scheme) were not presented as alternatives in the film. Instead we used a between-subject experimental design varying the film's ending and informing each group participating in a study on a different PET deployed at store exits (see appendix 1). Following the respective film stimulus they received a second questionnaire asking them to evaluate the benefits of the RFID services they had just seen as well as the respective PET displayed to them. In particular, they had to decide on an 11-point differential scale whether they would want to use a complex PET (if they had seen one) or rather kill RFID chips at store exits. The judgements participants made on this scale have been taken as the dependent variable to test hypotheses 1 through 5. Study ① embedded the four PET variations mentioned above. Study ② only differentiated between the User Scheme and leaving chips unprotected. Table 1 gives an overview of the two studies conducted.

The independent variables investigated in study ① included the perceived usefulness of RFID after sales services, the anticipated ease of use of RFID, peer opinion and perceived control through the PET (in terms of information control through the PET, ease of use of the PET and helplessness despite the PET). In study ② the same constructs were measured (except for peer opinion) and in addition personal variables were controlled for, including personal attitudes towards new technologies, technical affinity and general privacy awareness. Appendix 2 details the items used to measure these constructs.

3.2 Materials and Apparatus

The film stimulus was developed with the goal to inform participants in a neutral way about RFID technology, its benefits and drawbacks. It started out by showing a future retail outlet with RFID based services and then proceeded to introduce some retail related after-sales benefits of the technology. The film material used was taken from several existing television documentaries on RFID and combined with a professionally synchronized audio track. The audio track's text was carefully developed and tailored to contain an equal number of positive and negative messages about the technology. It was spoken with a view to maintain maximum neutrality. Equally, the film stimulus contained no background music or any other emotionally biasing signals.

In study ①, the film stimulus presented the retailer's check-out and after-sales scenarios in four different versions. Film 1 suggested that RFID chips would be left fully functional when checking out of the supermarket allowing for seamless RFID services after sales, but also potential attacks on one's privacy. The use of UHF chips was presumed for this scenario informing participants of read ranges between five and eight metres. Film 2 suggested that RFID chips would be killed by the retailer's cashpoint and no after sales services were presented to the participants. The appreciation of RFID after sales services was tested in a hypothetical way in this set-up before the film was shown and without mentioning the technology. Film 3 showed and explained the User Scheme, visualized as a password protection scheme. Participants were briefed to believe that all chips would be simultaneously deactivated and thus be privacy preserving unless the owner of an object would switch RFID chips back on with his or her personal password. Film 4 showed a user specifying his privacy preferences with a mobile operator. The reader network would then exchange privacy preferences with the mobile phone agent. The phone serves as a kind of watchdog service in this scenario. The two films 3 and 4 contained an equal number of positive and negative messages about the technology. They varied only in the description of the functioning of the technology which was described in a highly neutral way. Appendix 1 contains images and the exact wording used in films 3 and 4.

The focus in study ② was to better understand the dynamics behind using a User Scheme PET. For this purpose, only films 1 and 3 were used. Neutrality towards RFID technology and it was evaluated and confirmed in this study for films 1 and 3 with a median judgement of 7 on an 11 point scale (with 1 = film is negative about RFID and 11 = film is positive about RFID technology).

4 Results

4.1 Quantitative Evaluation of PET Solutions

A first analysis of the usefulness perceptions of RFID after sales services shows that participants feel neutral to positive about them regardless of the PET employed (table 2). There is no significant difference in service evaluation between the user and the agent scheme. However, not knowing about RFID technology as an enabler of smart services yielded a significantly higher appreciation of them.

Respondents to films 3 and 4 were split into two groups depending on whether their usefulness ratings were above or below mean group average. It was then tested whether those with usefulness ratings above average would value the use of a respective PET more in comparison to the kill alternative than those with low usefulness ratings.

In accordance with hypotheses 1 and 2 participants with above average usefulness perceptions of RFID valued both the User and the Agent PET significantly higher than those with low average usefulness ratings. On the 11-point scale anchoring the opposing preference for rather killing (1) or rather using a complex PET (11) people appreciating RFID after sales services in the User Scheme scenario rated the PET on average at 5,61. Those expecting less benefits from RFID rated the User PET at 2,49 (p=.000). In the group where participants saw the Agent Scheme appreciators of RFID valued the complex PET at 4,44 while non-appreciators valued it at 2,26 (p=.002). These results suggest that the perception of usefulness of RFID after sales services is an important driver for preferring complex PETs over the kill solution. Yet, absolute judgements show that all participants clearly prefer to kill RFID tags at store exits rather than adopting any of the two complex PET solutions presented to them.

Table 2. Mean (m) usefulness ratings of RFID after sales services in study ① *

Usefulness of RFID based after-sales services	**User Scheme (m)**	**Agent Scheme (m)**	**kill Chips (m)**	**sig. (User vs. Agent)**	**sig. (User vs. kill Chips)**	**sig. (Agent vs. kill Chips)**
Replace goods without receipt	3,84	3,85	4,44	.909	.002	.002
Warranty access without receipts	3,89	4,05	4,63	.621	.000	.000
Outdoor product recommendations	2,61	2,84	3,1	.290	.021	.252
Add. product information access at home	3,64	3,80	4,37	.494	.000	.000
Durability display of goods by fridge	3,45	3,67	4,00	.353	.009	.032
Washing machine warning	3,61	3,5	4,20	.347	.002	.000
Recipe recommendations	3,49	3,46	3,82	.803	.145	.101
Medical cabinet alerts	3,99	4,02	4,20	.966	.110	.088
Medical cabinet reminders	3,73	3,69	4,27	.630	.006	.001
Average Service Appreciation	**3,58**	**3,65**	**4,11**			

*) usefulness was measured on a 5 point scale (1 = very unsavoury, 5 = very welcome).

Average preferences among the appreciators of RFID services suggest that the User Scheme is slightly more valued than the Agent Scheme. To investigate this tendency reflected in hypothesis 3 the author compared participants' average tendency to kill in the User Scheme with the one in the Agent Scheme. And indeed the kill approach is preferred more often when the Agent PET is the alternative (m=3.31) than when the User PET is the alternative (m=4.03). However, this difference is not significant (p=.273). Therefore, hypothesis 3 that Agent Scheme users will want to kill RFID tags more readily than those confronted with the User Scheme must be rejected.

This finding of indifference between the two complex PET solutions is also reflected in a more thorough analysis of control perceptions raised through the two PETs. The author hypothesized that the User Scheme would lead to higher perceptions of control than the Agent Scheme (hypothesis 4). The reasoning behind this hypothesis as outlined above was that in the User Scheme users initiate communication with the reader infrastructure and need to confirm individual transactions before they take place. In the Agent Scheme they delegate these initiation decisions to an agent. As table 3 shows none of the three aspects of PET control significantly varies between the two PET solutions. Hypothesis 4 therefore needs to be rejected. In absolute terms users feel helpless vis-à-vis the reader infrastructure regardless of the type of PET employed. And this is the case even though they anticipate both PETs to be quite easy to use (which was suggested by the two films). Furthermore, they perceive information control on a medium level.

Table 3. Mean (m) control ratings in the experimental groups (study ①)

CONTROL MEASURES	Average Evaluation of the PET (m)		
	User PET	Agent PET	sig.
Ease of Use of PET	4,09	3,78	.052
Information through PET	3,28	3,40	.480
Helplessness despite PET	4,07	4,35	.112

Finally, we wanted to understand the relative importance of control, usefulness, ease of use as well as personal variables for preferring one ore the other PET scheme. For this purpose multiple regression analysis was conducted. Table 4 gives an overview of the results obtained.

All three regression models summarized in table 4 displayed significant F-Values proving that for each model the observed constructs have some systematic relationship with the decision to use a complex PET rather than kill the chip. The adjusted R^2 values (coefficients of determination) indicate that 40% to 48% of the variance in opting for a complex PET can be explained by the constructs included in the analyses. This level of variance explanation is quite satisfactory seen that there are potentially many factors for which the experimenters could not control. For example, participants' prior experience with remembering passwords or using mobile phone functionality, identity theft incidents, retailer trust, etc. could all influence the judgement in favour or against a complex PET. Since it is impossible to control for all of these factors explaining between 40 and 48% of the variance seems a satisfying result.

A revealing result of the regression models is that the reasons to opt for one or the other complex PET are not identical. When participants opt in favour of the User PET what counts for them most is the perception of usefulness of RFID after sales services. In contrast, participants who saw the Agent Scheme scenario seem to follow a different rationale. They opt for the complex Agent PET if their peers are in favour of using RFID. In both groups a perception of helplessness despite PET existence leads to a general tendency to reject both complex PETs. The more helpless users feel despite the User or Agent PET, the more they want to kill RFID tags. Mixed evidence was found on information properties of PETs and their effects on PET adoption. For the User PET information control seems to play a role, yet the direction of influence is unclear from the current analysis. For the Agent PET, in contrast, information control does not seem to play a role for adoption. It may be speculated that this is the case, because Agent PETs do not regularly inform users about read-outs. However, for this construct, as well as for peer opinion internal factor consistency (see α values) was mediocre and therefore do not allow making a very final judgement on the reliable influence of these constructs.

When personal variables were added to explain the preference for the kill function or the User PET in study ② it turned out that neither attitudes towards new technologies or technical affinity nor privacy concerns play a significant role for explaining peoples' judgement for PET usage or kill. Equally trust in the retailer was controlled for an yielded no impact on the adoption of PETs.

Table 4. Regression analyses: Divers for preferring the kill-function over a complex PET*

	Study ①								**Study ②**			
PET scenario	**User PET**				**Agent PET**				**User PET**			
Dependent Variable	Rather kill or rather use a PET scheme? (11-point scale: 1=kill, 11=PET)											
			Mean	**SD**			**Mean**	**SD**			**Mean**	**SD**
			4,03	3,15			3,31	2,55			4	3,13
Adjusted R^2 →			**.476**				**.396**				**.411**	
Independent Variables ↓	**no of items**	**α**	**ß**	**Sig.**	**no of items**	**α**	**ß**	**Sig.**	**no of items**	**α**	**ß**	**Sig.**
Constant			3,963				3,285				3.991	
Peer Opinion	2	.740	.145	.194	2	.468	**.438**	**.003**	2	-	-	-
Ease of use of RFID	3	.880	.238	.068	3	.785	.220	.255	3	.816	(-).010	.902
Usefulness of RFID	9	.929	**.323**	**.005**	9	.878	.036	.824	9	.886	**.413**	**.000**
Ease of use of PET	3	.881	(-).176	.164	3	.915	(-).082	.647	3	.809	.036	.629
Information PET	3	.837	**(-).335**	**.004**	3	.836	.144	.224	4	.773	**.146**	**.027**
Helplessness PET	2	.650	**(-).218**	**.019**	2	.579	**(-).347**	**.007**	4	.729	**(-).210**	**.003**
Attitude new technologies	-	-	-	-	-	-	-	-	4	.569	.001	.990
Technical Affinity	-	-	-	-	-	-	-	-	3	.798	.076	.220
Privacy Profile Aware	-	-	-	-	-	-	-	-	6	.877	.038	.513
Privacy Identity Aware	-	-	-	-	-	-	-	-	4	.821	.049	.384

The results suggest that in contrast to hypothesis 5 the two RFID PETs are not judged upon by a common set of acceptance factors. Depending on the PETs' interaction design different adoption parameters are determinative for preferring it over the kill option. Equally, hypothesis 6 can only be partially confirmed. Privacy awareness and general attitudes toward technology do not seem to be determinative for preferring one or another PET.

4.2 Qualitative Evaluation of PET Solutions

A final step in the analysis of PET perception was an attempt to understand why the large majority of participants generally prefer to kill RFID chips at store exits and what drives a smaller portion of users to instead opt for a more complex PET. In order to investigate this issue, participants in study ② were asked to explain their judgment for or against the User PET vis-à-vis the kill option. Explanations were given in a free text format (open question) by 175 out of the 208 participants in the User PET study. The author analyzed the reasoning for preferring a complex PET or rather killing tags with the help of a content analysis [30]. Each answer typically had one main *theme* (reason) for why a participant would judge for the User PET or rather favour the killing of RFID tags. These reasons are summarized in table 5.

Table 5. Main themes for participants when opting for a User PET or instead kill tags

Reasons given for Preferring Kill Function over User PET (or vice versa)	**Kill (1-4)**	**Neutral (7-5)**	**User PET (11-8)**
	108	32	35
	62%	18%	20%
mistrust "security" of password scheme	27	6	1
feeling to still be "recognized" somehow	17	0	0
unspecified "misuse"	15	0	0
maximum protection through kill	9	0	0
desire to not be controlled/feel in "control"	8	1	0
uncertainty towards any privacy solution	0	9	1
TRUST related reasons against User PET	*76 (70%)*		
consequences for society	23	2	0
other	6	0	1
transaction cost of the password scheme	3	1	0
lost RFID benefit	0	11	16
appreciation of the PET	0	1	8
transaction cost to kill	0	1	5
unconcerned	0	0	1
passive resignation	0	0	2

175 out of the 208 participants who viewed the User PET scenario in study 2 (84%) gave a reason for why they rather preferred the kill function over the User PET or vice versa. Out of the 108 (62%) participants who were in favour of killing RFID tags 70% described some feeling of mistrust in the password PET. They expressed their belief that passwords could be "hacked" or that "security" is generally weak. They also feared some unspecified "misuse" or that they would still be recognized or scanned somehow. These findings clearly hint to the importance of security visibility when engineering RFID PETs. The second largest group of those who want to rather kill RFID tags (21%) are people who seem to base their judgements on the consequences of RFID they fear for themselves and for society at large. They mention "privacy" and "data protection", but also express rejection of marketing practices, surveillance ("Big Brother") and the course of a "chipped" society.

Subjects which were in favour of using the User PET mostly based their decision on the fact that they appreciated RFID benefits and liked the idea to have a "choice". Some participants (18%) finally were stuck in the middle in seeing RFID benefits on one side, but equally mistrusting the PET solution.

5 Discussion, Conclusions and Limitations

The main finding of the presented research is that complex PETs as they are envisioned today by many UbiComp privacy researchers are highly likely to run into acceptance problems with users. The majority of consumers seem to want to kill RFID chips at store exits rather than using any of the complex technical solutions presented to them. This is the case even though the films suggested high ease of use and seamless privacy management. The desire to kill RFID tags is ***not*** due to the fact that consumers do not comprehend or value the benefits of RFID services (as is often argued by industry today). In contrast, consumers do value the service spectrum which can be realized through RFID. But they are willing to forgo these benefits in order to protect their privacy. This highlights the importance of the topic of privacy for the UbiComp research community.

Content analysis suggests that what users are looking for are highly trustworthy and straight forward solutions to privacy. Solutions that leave no room for speculation about security levels as passwords may be hacked or network protocols may be intransparent. Instead signalling security and trust to users through respective interface design may be very relevant for privacy engineering in UbiComp.

A further finding of the study is that the User Scheme does not seem to be superior to the Agent Scheme. Despite user initiation of network communication the PET does not induce higher levels of perceived control. However, the results from regression analyses suggest that User Scheme appreciation can be improved by working on the PET itself: Information control provided through the User PET seems to directly influence its appreciation. Thus, if users have the impression that they have a direct choice in a context to activate chips on an informed basis then they are also more likely to prefer the User PET over the kill option. Content analysis furthermore revealed that information provided here should include reassuring messages about the security level achieved by the PET. Therefore, research in security visibility as currently driven by the W3C may be of high interest in the UbiComp community [31].

In contrast, Agent PETs do not seem to be based on the same dynamics. If network agents organize users' privacy in a largely autonomous way, then people seem to rely more on the recommendations of peers when deciding not to kill. If peers say that RFID is fine to use, then trust which is placed in the Agent PET seems to increase.

A limitation of the present research is that it only showed one type of User PET which was based on passwords. People often attribute problems to passwords, both in handling them and in terms of security [32]. Different results may have been obtained if the User Scheme film had shown, for example, biometrics as the authentication mechanism. Thus, the empirical investigation presented here is really only viable for the concrete technological scenarios shown to the participants and not sufficient to deduct conclusions about user initiated communications in general. More research is needed for generalize the findings.

Furthermore, film scenarios may bear the methodological risk of bias. We made an effort to minimize bias and controlled for the neutrality of the film material. Yet, we can hardly measure how strongly people were impacted by the sole mentioning of privacy issues. Privacy is a subject of prime importance to Germans and it may be that this cultural background has led to stronger results in favour of killing RFID chips than may be the result if the study was replicated in other cultures. Furthermore, it is well known that behavioural intentions as expressed in such surveys, even though being strong indicators for actions taken cannot be equalized with actual behavior [28, 33, 34] (mean correlations are around .53 according to [35]).

An advantage of using film scenarios is the wide spectrum of services that can be shown as well as the visualization of service and protection alternatives. Drawbacks of usability studies with real prototypes can be avoided in this way. For example, malfunctioning of prototypes, difficulties of use, very small sample sizes, etc. The methodological approach taken in the studies presented here therefore is new. Yet, it may be interesting for UbiComp researchers in general, because they have to envision what exactly their applications will look like to future users and test alternatives in advance. In this way potential acceptance problems may be detected and corrected early in the development cycle.

References

1. Fusaro, R.: None of Our Business. Harvard Business Review, 33–44 (2004)
2. Smith, J.H., Milberg, J., Burke, S.: Information Privacy: Measuring Individuals' Concerns About Organizational Practices. MIS Quarterly 20(2), 167–196 (1996)
3. Jannasch, U., Spiekermann, S.: RFID: Technologie im Einzelhandel der Zukunft: Datenentstehung, Marketing Potentiale und Auswirkungen auf die Privatheit des Kunden, Lehrstuhl für Wirtschaftsinformatik, Humboldt Universität zu Berlin: Berlin (2004)
4. Berthold, O., Guenther, Spiekermann, S.: RFID Verbraucherängste und Verbraucherschutz. Wirtschaftsinformatik, Heft 6 (2005)
5. FoeBuD e.V. (ed.): Positionspapier über den Gebrauch von RFID auf und in Konsumgütern, FoeBuD e.V.: Bielefeld (2003)
6. Duce, H.: Public Policy: Understanding Public Opinion, A.-I. Center, Massachusetts Institute of Technology. MIT, Cambridge, USA (2003)
7. Auto-ID Center (ed.): 860 MHz – 930 MHz Class 1 Radio Frequency (RF) Identification Tag Radio Frequency & Logical Communication Interface Specification, EPCGlobal, Cambridge, Massachusetts, USA (2004)

8. Sarma, S., Weis, S., Engels, D.: RFID Systems, Security & Privacy Implications, A.-I. Center. Massachusetts Institute of Technology. MIT, Cambridge, USA (2002)
9. Auto-ID Center, (ed.): Technology Guide. Massachusetts Institute of Technology, MIT, Cambridge, USA (2002)
10. GCI (ed.): Global Commerce Initiative EPC Roadmap, G.C. Initiative and IBM (2003)
11. Auto-ID Center, (ed.): EPC-256: The 256-bit Electronic Product Code Representation. Massachusetts Institute of Technology, MIT, Cambridge, USA (2003)
12. Auto-ID Center, (ed.): EPC Information Service - Data Model and Queries. Massachusetts Institute of Technology, MIT, Cambridge, USA (2003)
13. Auto-ID Center, (ed.): Auto-ID Object Name Service (ONS) 1.0. Massachusetts Institute of Technology, MIT, Cambridge, USA (2003)
14. Engels, D.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In: Hutter, D., Müller, G., Stephan, W., Ullmann, M. (eds.) Security in Pervasive Computing. LNCS, vol. 2802, Springer, Heidelberg (2004)
15. Engberg, S., Harning, M., Damsgaard, C.: Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience. In: Proceedings of the Second Annual Conference on Privacy, Security and Trust, New Brunswick, Canada (2004)
16. Spiekermann, S., Berthold, O.: Maintaining privacy in RFID enabled environments - Proposal for a disable-model. In: Robinson, P., Vogt, H. (eds.) Privacy, Security and Trust within the Context of Pervasive Computing, Springer Verlag, Vienna, Austria (2004)
17. Inoue, Y.: RFID Privacy Using User-controllable Uniqueness. In: Proceedings of the RFID Privacy Workshop, Massachusetts Institute of Technology, MIT, Cambridge, MA, USA (2004)
18. Floerkemeier, C., Schneider, R., Langheinrich, M.: Scanning with a Purpose - Supporting the Fair Information Principles in RFID Protocols. In: Murakami, H., Nakashima, H., Tokuda, H., Yasumura, M. (eds.) UCS 2004. LNCS, vol. 3598, Springer, Heidelberg (2005)
19. Langheinrich, M.: A Privacy Awareness System for Ubiquitous Computing Environments. In: Borriello, G., Holmquist, L.E. (eds.) UbiComp 2002. LNCS, vol. 2498, Springer, Heidelberg (2002)
20. Christian, M., Floerkemeier, C.: Making Radio Frequency Identification Visible – A Watchdog Tag. In: Proceedings of the 5th Annual IEEE International Conference on Pervasive Computing and Communications, New York (2007)
21. Stajano, F.: Security for Ubiquitous Computing. John Wiley & Sons, Chichester, UK (2002)
22. Platform for Privacy Preferences (P3P) Project, W3C (2006)
23. Juels, A., Rivest, R., Szydlo, M.: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In: Proceedings of the 10th Annual ACM CCS, ACM Press, New York (2003)
24. Karjoth, G., Moskowitz, P.A.: Disabling RFID Tags with Visible Confirmation: Clipped Tags are Silenced. In: Proceedings of the ACM Workshop on Privacy in the Electronic Society, ACM Press, Alexandria, VA, USA (2005)
25. Spiekermann, S.: Perceived Control: Scales for Privacy in Ubiquitous Computing. In: Acquisti, A., De Capitani di Vimercati, S., Gritzalis, S., Lambrinoudakis, C. (eds.) Digital Privacy: Theory, Technologies and Practices, Taylor and Francis, New York (2007)
26. Fishbein, M., Ajzen, I.: Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research. Addison-Wesley, Reading, MA, USA (1975)

27. Ajzen, I.: From intentions to actions: A theory of planne behavior. In: Kuhi, J., Beckmann, J. (eds.) Action - control: From cognition to behavior, pp. 11–39. Springer, Heidelberg (1985)
28. Ajzen, I., Fishbein, M.: The Influence of Attitudes on Behavir. In: Albarracin, D., Johnson, B.T., Zanna, M.P. (eds.) The Handbook of Attitudes on Behavior, pp. 173–221. Erlbaum, Mahwah, New York (2005)
29. Rogers, E.: Diffusion of Innovations. The Free Press, New York (1995)
30. Kassarjian, H.H.: Content Analysis in Consumer Research. Journal of Consumer Research 4(1), 8–18 (1977)
31. W3C, (ed.): Web Security Experience, Indicators and Trust: Scope and Use Cases, W3C Working Draft (25 May 2007)
32. Adams, A., Sasse, A.: Users are not the enemy - Why users compromise computer security mechanisms and how to take remedial measures. Communications of the ACM 42(12), 40–46 (1999)
33. Berendt, B., Guenther, O., Spiekermann, S.: Privacy in E-Commerce: Stated Preferences vs. Actual Behavior. Communications of the ACM 48(4) (2005)
34. Sheeran, P.: Intention-behavior relations: A conceptual and empirical review. In: Stroebe, W., Hewstone, M. (eds.) European Review of Social Psychology, pp. 1–36. Wiley, Chichester, UK (2002)
35. Trafimow, D.: Evidence that perceived behavioural control is a multidimensional construct: Perceived control and perceived difficulty. British Journal of Social Psychology 41, 101–121 (2002)