Privacy Enhancing Technologies for RFID in Retail- An Empirical Investigation

UbiComp'07, Innsbruck, September 2007

A new book ☺! by Sarah

HUMBOLDT-UNIVERSITÄT ZU BERLIN

HABILITATION

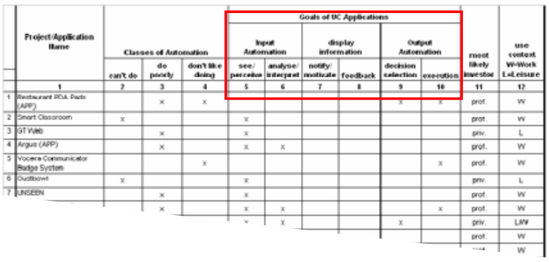
User Control in Ubiquitous Computing: Design Alternatives and User Acceptance

Zur Erlangung des akademischen Grades
Venia Legendi

can be retrieved from:www.wiwi.hu-berlin.de/~sspiek

UC applications what are they all about? 93% about input automation…

Table 1: Ubiquitous Computing applications: A snapshot of prototypes from 2003-2005



	Project/Application Name	Classes of Automation			Goals of UC Applications						most likely investor	use context W=Work L=Leisure
					Input Automation		display information		Output Automation			
		can't do	do poorly	don't like doing	see/ perceive	analyse/ interpret	notify/ motivate	feedback	decision selection	execution		
	1	2	3	4	5	6	7	8	9	10	11	12
1	Restaurant PDA Pads (APP)		x	x					x	x	prof.	W
2	Smart Classroom	x			x						prof.	W
3	GT Web		x		x						priv.	L
4	Argus (APP)		x		x	x					prof.	W
5	Vocera Communicator Badge System			x						x	prof.	W
6	Outlbowl	x			x						priv.	L
7	UNSEEN		x		x						prof.	W
			x		x	x				x	prof.	W
					x	x			x		priv.	L/W
											prof.	W
											[illegible]	W

Spiekermann, S., "User Control in Ubiquitous Computing: Design Alternatives and User Acceptance", Sept. 2007

Privacy in Interaction with Smart Devices is not relevant for people in their purchase and use intentions.

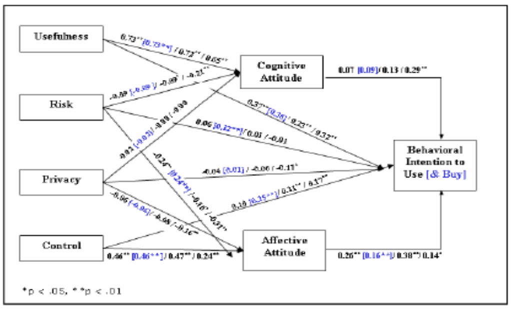


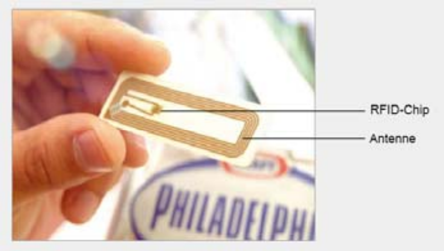
Figure 24: UC-AM: relationships and path coefficients (fridge use [buy] / ISA / garage scenario)

Spiekermann, S., "User Control in Ubiquitous Computing: Design Alternatives and User Acceptance", Sept. 2007

Agenda

- **Introduction to RFID and the Privacy Issue**
- Qualitative Research Results: User Concerns over RFID
- Privacy Enhancing Technologies (PETs) for RFID
- PET Acceptance: Is the Kill Function a Dead-End?

RFID tags are one important component of the *Intelligent Infrastructure* or Ubiquitous Computing Landscape.



RFID tags bear tremendous potential for supply chain optimization.

Experiences made by Metro Group

- **Reduction of labor cost (~ 11%)**
- **Reduction of losses along the supply chain (~ 11-18%)**
- **Reduction of Out-of-Stock Situations (9 - 14%)**

RFID also has the potential to revolutionize marketing at the POIS.

- **Product Portfolio**
  - More precise sales analysis through enhanced numbering system use
  - Person – product attribution
    - … through combination with video systems
    - … through enhanced numbering system in combination with loyalty cards
  - Optimization of product qualities through serial number tracking
- **Price**
  - Facilitation of price differentiation through intelligent shelves
- **Promotion**
  - More precise measurement of advertisment effectiveness: ad pricing based on consumer attention instead of eye-balls.
  - Personalized recommendations based on „attention“ information
- **Product placement and shop-floor design**
  - Optimization of shop-floor design through enhanced movement tracking

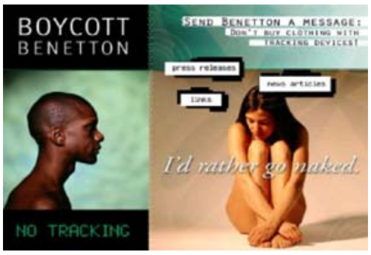
* Working Paper: Spiekermann und Jannasch, April 2004

RFID triggers strong emotions among privacy rights organizations.

future STORE
STOP RFID
peRFIDe!!!
METRO
Ist auch Ihre Payback-Karte schon verwanzt?
RFID gefährdet Ihre Privatsphäre

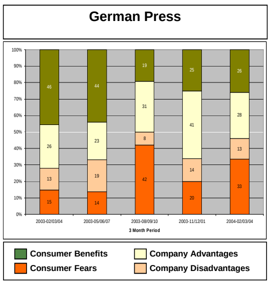
Public Outcry in Rheinberg (Germany)

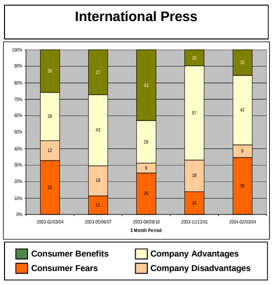
Some companies have put RFID projects on hold fearing consumer backlash on privacy issues.



US Campaign by Caspian against benetton

The press picks up privacy rights arguments.





…and Harvard writes Case Studies…

HBR: “None of our Business?”
by Roberta A. Fusaro

Agenda

- Introduction to RFID and the Privacy Issue
- **Qualitative Research Results: User Concerns over RFID**
- Privacy Enhancing Technologies (PETs) for RFID
- PET Acceptance: Is the Kill Function a Dead-End?

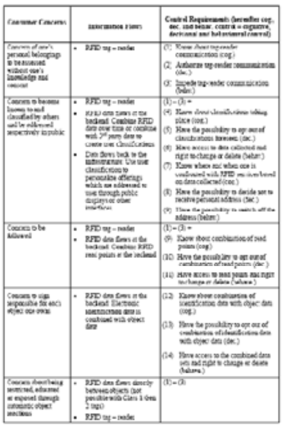
What are major consumer fears associated with RFID?

Focus Group Results

- Concern of one's personal belongings to be assessed without one's knowledge and consent
- Concern to become known to and classified by others
- Concern to be followed
- Concern to sign responsible for each object one owns
- Concern about being restricted, educated or exposed through automatic object reactions

„…something is being done with me that I cannot really control and grasp and this is what I am afraid of.“ (group 3, S. 32)

Spiekermann, S., "User Control in Ubiquitous Computing: Design Alternatives and User Acceptance", Sept. 2007



Consumer Concerns	Information Flows	Control Requirements (hereafter cog., dec. and behav. control = cognitive, decisional and behavioural control)
Concern of one's personal belongings to be assessed without one's knowledge and consent	• RFID tag – reader	(1) Know about tag-reader communication (cog.) (2) Authorise tag-reader communication (dec.) (3) Impede tag-reader communication (behav.)
Concern to become known to and classified by others and be addressed respectively in public	• RFID tag – reader • RFID data flows at the backend: Combine RFID data over time or combine with 3rd party data to create user classifications • Data flows back to the infrastructure: Use user classification to personalize offerings which are addressed to user through public displays or other interfaces	(1) – (3) + (4) Know about classifications taking place (cog.) (5) Have the possibility to opt out of classifications foreseen (dec.) (6) Have access to data collected and right to change or delete (behav.) (7) Know where and when one is confronted with RFID services based on data collected (cog.) (8) Have the possibility to decide not to receive personal address (dec.) (9) Have the possibility to switch off the address (behav.)
Concern to be followed	• RFID tag – reader • RFID data flows at the backend: Combine RFID read points at the backend	(1) – (3) + (9) Know about combination of read points (cog.) (10) Have the possibility to opt out of combination of read points (dec.) (11) Have access to read points and right to change or delete (behav.)
Concern to sign responsible for each object one owns	• RFID data flows at the backend: Electronic identification data is combined with object data	(12) Know about combination of identification data with object data (cog.) (13) Have the possibility to opt out of combination of identification data with object data (dec.) (14) Have access to the combined data sets and right to change or delete (behav.)
Concern about being restricted, educated or exposed through automatic object reactions	• RFID data flows directly between objects (not possible with Class 1 Gen 2 tags) • RFID tag – reader	(1) – (3)

Control Requirements for RFID PETs:

to provide for
- cognitive
. decisional
- behavioural
CONTROL

Spiekermann, S., "User Control in Ubiquitous Computing: Design Alternatives and User Acceptance", Sept. 2007

Agenda

- Introduction to RFID and the Privacy Issue
- Qualitative Research Results: User Concerns over RFID
- **Privacy Enhancing Technologies (PETs) for RFID**
- PET Acceptance: Is the Kill Function a Dead-End?

PETs for RFID: A Snapshot of the Literature

	2002	2003	2004	2005	2006	2007 (until June)	Total
Number of papers published on security and privacy in RFID systems on Gildas Avoine's Site	1	11	23	59	66	17	177
Number of papers containing technical proposals to control information flow between tag and reader	1	8 (72%)	17 (74%)	32 (54%)	52 (79%)	13 (76%)	123 (69%)
… of these, those which describe their motivation as protecting *end-user* privacy	0	4 (50%)	14 (82%)	25 (78%)	22 (42%)	6 (46%)	71 (57%)
dealing with…							
RFID Kill Function							
User Scheme		1	2	2	0	0	5
Agent Scheme		1	1	3	3	0	8
On-tag Scheme		2	11	20	19	6	58

Spiekermann, S., "User Control in Ubiquitous Computing: Design Alternatives and User Acceptance", Sept. 2007

Some notes on the Class1/Gen2 tags' kill-function…

"If you consider that RFID tags represent the future of computing technology, this proposal [the kill function] becomes as absurd as permanently deactivating desktop PCs to reduce the incidence of computer viruses and phishing"
(p. 92 in (Rieback, Gaydadjiev et al. 2006)).

Spiekermann, S., "User Control in Ubiquitous Computing: Design Alternatives and User Acceptance", Sept. 2007

Encryption? Not really…

Beyond password management…

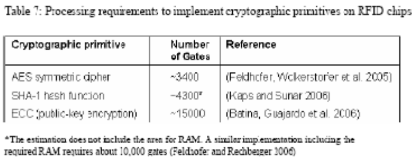


Table 7: Processing requirements to implement cryptographic primitives on RFID chips

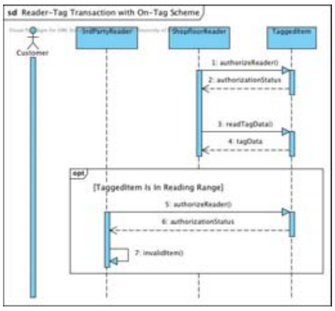
Cryptographic primitive	Number of Gates	Reference
AES symmetric cipher	~3400	(Feldhofer, Wolkerstorfer et al. 2005)
SHA-1 hash function	~4300*	(Kaps and Sunar 2006)
ECC (public-key encryption)	~15000	(Batina, Guajardo et al. 2006)

*The estimation does not include the area for RAM. A similar implementation including the required RAM requires about 10,000 gates (Feldhofer and Rechberger 2006)

(Juels and Weis 2005): "One might assume that Moore's Law will eventually enable RFID tags and similar devices to implement standard cryptographic primitives like AES. But there is a countervailing force: Many in the RFID industry believe that pricing pressure and the spread of RFID tags into ever more cost-competitive domains will mean little effective change in tag resources for some time to come, and thus a pressing need for new lightweight primitives" (p. 294).

Spiekermann, S., "User Control in Ubiquitous Computing: Design Alternatives and User Acceptance", Sept. 2007

…none of the control requirements is fulfilled.



Spiekermann, S., "User Control in Ubiquitous Computing: Design Alternatives and User Acceptance", Sept. 2007

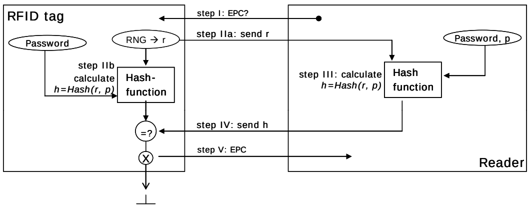
User/Password Model: Direct User Control

- RFID chips are sealed (deactivated) at the store exit with a privacy password.
- This deactivation is done seamlessly and simultaneously for all products (no transaction cost)
- The password scheme is supposed to be secure.

- If services are sought on the basis of RFID chips after purchase, the privacy password serves as authorization.
- The consumer initiates service use.

–Spiekermann, S., Berthold O., "Maintaining privacy in RFID enabled environments - Proposal for a disable-model", in: Privacy, Security and Trust within the Context of Pervasive Computing, Hrsg. P. Robinson, H. Vogt, W. Wagealla, The Kluwer International Series in Engineering and Computer Science, Springer Verlag, 2005

The Password Model



–Spiekermann, S., Berthold O., "Maintaining privacy in RFID enabled environments - Proposal for a disable-model", in: Privacy, Security and Trust within the Context of Pervasive Computing, Hrsg. P. Robinson, H. Vogt, W. Wagealla, The Kluwer International Series in Engineering and Computer Science, Springer Verlag, 2005

Network (Agent) Model: Control is delegated

- RFID chips are generally left on to respond to network requests.
- Access to chips is managed via privacy preferences stored on the network.
- A user specifies these privacy preferences in written form with a mobile operator.

- Privacy preference management is then done automatically via the mobile phone.
- The mobile phone serves as a privacy buffer.
- It is asked by readers whether tags can be read out or not.
- It has the power to deny access.

Spiekermann, S., "User Control in Ubiquitous Computing: Design Alternatives and User Acceptance", Sept. 2007

Agenda

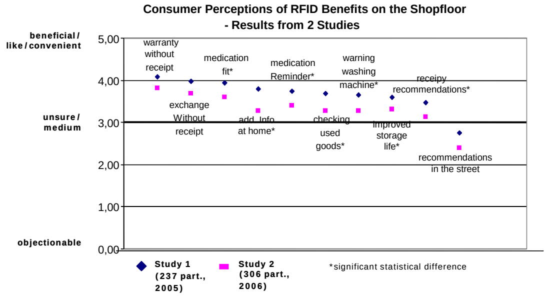
- Introduction to RFID and the Privacy Issue
- Qualitative Research Results: User Concerns over RFID
- Privacy Enhancing Technologies (PETs) for RFID
- **PET Acceptance: Is the Kill Function a Dead-End?**

Participants of 2 susequent studies on RFID acceptance

		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	

Spiekermann, S., "User Control in Ubiquitous Computing: Design Alternatives and User Acceptance", Sept. 2007 &
Spiekermann, S, "Privacy Enhancing Technologies for RFID in Retail- An Empirical Investigation" , UbiComp Paper, 2007

RFID based after-sales services are seen quite positive by participants.



– Günther, O., Spiekermann, S. , "RFID And The Perception of Control: The Consumer's View", Communications of the ACM (CACM), Vol. 48, No. 9, September 2005

In a pre-study control items were ranked and categorized.

Rank	Index	Question text *(1 = fully agree ... 5 = do not agree at all)*	Category
1	POW 1	I feel that I can steer the intelligent environment in a way I feel is right.	Power
2	POW 2	Thanks to <the PET> the electronic environment and its reading devices will have to subdue to my will.	
5	POW 3	Due to <the PET> I perceive perfect control over the activity of my chips.	
3	CON 1	Thanks to <the PET> I could determine myself whether or not I'll interact with the intelligent environment.	Contingency
7	CON 2	Through <the PET>, services are put at my disposition when I want them.	
6	H 2	I could imagine that if the electronic environment set out to scan me, it would be able to do so despite <the PET>.	Helplessness
10	H 1	<The PET> will finally not be able to effectively protect me from being read by the electronic environment.	
8	COI 1	Due to <the PET> it is still my decision whether or not the intelligent environment recognizes me.	Choice
4	COI 2	Through <the PET> I finally have the choice whether or not I am being scanned or not	
9	IC 1	Through <the PET> I would always be informed of whether and in what form the electronic environment recognizes me.	Information
11	IC 2	Using <the PET> I would always know when and by whom I have been read out.	
*	EUP 1	To learn to use <the PET> would be easy for me.	Ease-of-use
*	EUP 2	It would be easy for me to learn skillful use of <the PET>.	
*	EUP 3	I would find <the PET> easy to use.	
*	EUP 4	Due to <the PET> the information exchange between my chips and reading devices would be clearly defined.	

–Spiekermann, S., "User Control in Ubiquitous Computing: Design Alternatives and User Acceptance", Sept. 2007

Control through PET use is neither perceived when deploying the Agent Scheme nor when using the User Scheme.

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

– Günther, O., Spiekermann, S. , "RFID And The Perception of Control: The Consumer's View", Communications of the ACM (CACM), Vol. 48, No. 9, September 2005

73% of participants want to see RFID chips destroyed rather than taking advantage of the benefits. The trend is reenforced the more education people have.

F48: Die vorangegangenen Fragen und der Film zeigen, dass RFID Technologie Nachteile und Vorteile für den Verbraucher mit sich bringt. Natürlich wäre statt des Passwortschutzes denkbar, alle Chips am Ladenausgang vollständig zu vernichten. Was ist Ihre Gesamteinschätzung zu dieser Frage? Bitte markieren Sie Ihre Tendenz auf einer Skala:

□ □ □ □ □ □ □ □ □ □ □

Chips vollständig vernichten — **Chips mit Passwort versehen**

	Tendency to reject PET (1–5)	Undecided (6)	Tendency to use PET for advantage (7–11)
User Model with IB	69.9% *82.9%**	8.2% *4.9%**	21.9% *12.2%**
Network Model without IB	78.2% *71.4%*	9.1% *11.4%*	12.7% *17.1%*
Gesamt with IB	73.4% *77.6%*	8.6% *7.9%*	18.0% *14.5%*

Deactivation vs. PET. The numbers in italics represent the top 60% of the panel with respect to education.
The asterisk* denotes a significant difference of technology perception due to education.

– Günther, O., Spiekermann, S. , "RFID And The Perception of Control: The Consumer's View", Communications of the ACM (CACM), Vol. 48, No. 9, September 2005

What drives the preferences for using Agent and User PETs vis-à-vis the kill-function?

	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 R² →			.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

Spiekermann, S., "User Control in Ubiquitous Computing: Design Alternatives and User Acceptance", Sept. 2007 &
Spiekermann, S, "Privacy Enhancing Technologies for RFID in Retail- An Empirical Investigation" , UbiComp Paper, 2007