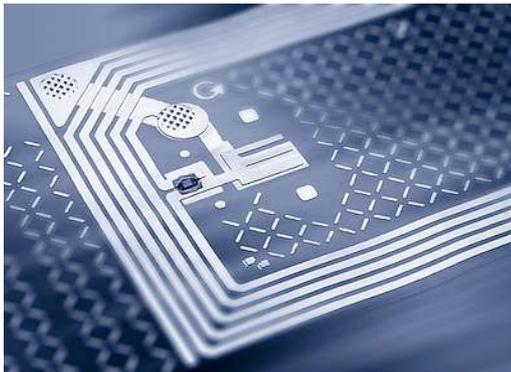


Pre-Publishing Draft

**User Control in
Ubiquitous Computing:
Design Alternatives and
User Acceptance**



Institute of Information Systems
Humboldt-Universität zu Berlin

Dr. Sarah Spiekermann
sspiek@wiwi.hu-berlin.de



CONTENTS

LIST OF TABLES	4
LIST OF FIGURES	5
EXECUTIVE SUMMARY	6
PREFACE.....	8
1 INTRODUCTION.....	11
2 UBIQUITOUS COMPUTING: THE AUTOMATION OF EVERYDAY LIFE AND THE ROLE OF CONTROL.....	15
2.1 WHAT IS UBIQUITOUS COMPUTING?	15
2.2 UBIQUITOUS COMPUTING AND THE AUTOMATION OF EVERYDAY LIFE	16
2.2.1 <i>Automation and Parallels to Ubiquitous Computing</i>	16
2.2.2 <i>Classifying Ubiquitous Computing Applications</i>	18
2.3 USER ACCEPTANCE OF AUTOMATION AND THE ROLE OF CONTROL	21
2.3.1 <i>Concept and Study of User Acceptance</i>	22
2.3.2 <i>Meaning of the Term ‘Control’</i>	23
2.3.3 <i>Acceptance Challenges of Input Automation and the Role of Control</i>	26
2.3.4 <i>Acceptance Challenges of Output Automation and the Role of Control</i>	32
2.3.5 <i>Conclusion: Is Automation Automatically a Good Thing?</i>	35
3 USER CONCERNS, TECHNICAL CHALLENGES AND CONTROL OPTIONS OVER AUTOMATED INFORMATION COLLECTION – THE CASE OF RFID	37
3.1 INTRODUCTION TO RFID	37
3.1.1 <i>The Many Forms of RFID</i>	38
3.1.2 <i>Information Infrastructures and Architectures for RFID</i>	39
3.1.3 <i>Benefits and Critiques of RFID</i>	39
3.2 INFORMATION COLLECTION CONCERNS OVER RFID	42
3.2.1 <i>Method: A Qualitative Approach to Elicit Consumer Concerns</i>	44
3.2.2 <i>Results: RFID Related Consumer Concerns</i>	45
3.2.3 <i>Discussion: Requirements for RFID Information Flow Control</i>	47

3.3	TECHNICAL FEASIBILITY OF CONSUMER CONCERNS.....	50
3.3.1	<i>Unauthorised Assessment of Belongings and Classification</i>	50
3.3.2	<i>Tracking of Individuals via their Objects</i>	51
3.3.3	<i>Making People Responsible for Objects</i>	53
3.3.4	<i>Being Restricted or Social Control through RFID</i>	54
3.4	TECHNICAL OPTIONS TO ADDRESS CONSUMER CONCERNS.....	56
3.5	MEASURING PERCEIVED CONTROL OVER RFID TAG-READER COMMUNICATION	66
3.5.1	<i>Dimensions of Perceived Control</i>	67
3.5.2	<i>Scale Development and Item Testing</i>	68
3.6	RFID PET ACCEPTANCE AND THE RELATIVE IMPORTANCE OF PERCEIVED CONTROL	72
3.6.1	<i>Method Used to Investigate User Perceptions of RFID PETs</i>	74
3.6.2	<i>Results: How do Users Respond to PETs for RFID?</i>	77
3.6.3	<i>A Qualitative Evaluation of PET Solutions</i>	79
3.6.4	<i>Conclusions on the Acceptance of PET Solutions</i>	81
3.7	CONCLUSION: INFORMATION COLLECTION WITH RFID.....	83
4	A UBIQUITOUS COMPUTING ACCEPTANCE MODEL AND THE ROLE OF CONTROL OVER AUTOMATED SYSTEM ACTIVITY	85
4.1	TECHNOLOGY ACCEPTANCE RESEARCH AND ITS TRANSFERABILITY TO UBIQUITOUS COMPUTING.....	85
4.2	CONCEPTUAL FRAMEWORK FOR A UBIQUITOUS COMPUTING ACCEPTANCE MODEL.....	87
4.2.1	<i>Hypotheses on the Drivers and Impediments of UC Acceptance</i>	87
4.2.2	<i>Method to Investigate the UC-Acceptance Model</i>	93
4.2.3	<i>Results: Fit and Strength of the UC-Acceptance Model</i>	96
4.2.4	<i>Discussion: The Value of UC-AM to Explain Service Acceptance</i>	100
4.2.5	<i>Implications of the UC- Acceptance Model for Practice</i>	103
4.3	ABOUT THE IMPORTANCE OF FUNCTION ALLOCATION FOR UC ACCEPTANCE.....	104
4.3.1	<i>Methodology: A Scenario Based Variation of Function Allocation</i>	107
4.3.2	<i>Results: Perceptions and Effects of Function Allocation</i>	108
5	CONCLUSION.....	112
6	REFERENCES.....	116
7	APPENDIX.....	129

LIST OF TABLES

Table 1: Ubiquitous Computing applications: A snapshot of prototypes from 2003-2005.....	20
Table 2: Objects of supervision and supervisor relationships in UC applications.....	29
Table 3: Exemplary application of automation levels to two UC scenarios.....	34
Table 4: RFID frequency bands and read ranges	38
Table 5: Consumer concerns, information flows and control requirements.....	49
Table 6: A snapshot of the scientific literature on RFID privacy and security	57
Table 7: Processing requirements to implement cryptographic primitives on RFID chips.....	60
Table 8: Questions measuring perceived control over RFID tag-reader communication	69
Table 9: Reliability indicators of control scale (group 1: User Scheme).....	71
Table 10: Reliability indicators of control scale (group 2: Agent Scheme)	71
Table 11: Experimental groups and demographics	75
Table 12: Mean (m) usefulness ratings of RFID after sales services in study ①	77
Table 13: Mean (m) control ratings in the experimental groups (study ①).....	78
Table 14: Regression analyses: Divers for preferring the kill-function over a complex PET.....	79
Table 15: Main themes for participants when opting for a User PET instead of killing tags	80
Table 16: Trust Design Guidelines for E-Commerce Sites	82
Table 17: Outer loadings of indicators on the UC - AM constructs	97
Table 18: Discriminant validity of measures scenario 1: intelligent fridge (intention to use).....	97
Table 19: Discriminant validity of measures scenario 1: intelligent fridge (intention to buy)	97
Table 20: Discriminant validity of measures scenario 2: ISA	97
Table 21: Discriminant validity of measures scenario 3: automatic garage service	98
Table 22: R ² results for TAM versus UC-AM	99
Table 23: Total effects of model constructs on intention to use or buy a UC Service.....	102
Table 24: Demographics of two samples of participants of the 2 nd UC Acceptance Study	108
Table 25: Differences in constructs between low- and high control groups (online sample)	109
Table 26: Differences in constructs between low- and high control groups (paper sample).....	111

LIST OF FIGURES

<i>Figure 1: The scope of automation (p.10 in (Sheridan 2002)</i>	<i>17</i>
<i>Figure 2: Four stages of automation with distinct automation levels</i>	<i>19</i>
<i>Figure 3: Design rules for feedback to promote control</i>	<i>23</i>
<i>Figure 4: Model of supervisory control in classical automation (a) and adaptation to UC (b).....</i>	<i>25</i>
<i>Figure 5: Argus Project: Video based analysis of near shore environments.....</i>	<i>31</i>
<i>Figure 6: The goal of automation</i>	<i>35</i>
<i>Figure 7: Consumer perceptions of after-sales benefits of RFID</i>	<i>40</i>
<i>Figure 8: The Impact on privacy from RFID vs. other technologies.....</i>	<i>43</i>
<i>Figure 9: Automatic check-out of products tagged with RFID chips (Metro Group in 2004)</i>	<i>44</i>
<i>Figure 10: A Password based deactivator station for RFID tags.....</i>	<i>44</i>
<i>Figure 11: Attack-tree: Assessing objects tagged with an UHF RFID tag.....</i>	<i>50</i>
<i>Figure 12: The Structure of the Electronic Product Code (EPC).....</i>	<i>51</i>
<i>Figure 13: Attack-tree: Tracking persons</i>	<i>52</i>
<i>Figure 14: Attack- tree: Making people responsible for objects.</i>	<i>54</i>
<i>Figure 15: Attack-tree: Implementing social controls on the basis of RFID-labelled items</i>	<i>55</i>
<i>Figure 16: UML sequence diagram: RFID based communication in a mall, ‘On-tag’ Scheme</i>	<i>59</i>
<i>Figure 17: Challenge-response process for RFID tag-reader communication</i>	<i>59</i>
<i>Figure 18: UML Sequence Diagram: RFID based communication in an intelligent mall, Agent Scheme.....</i>	<i>62</i>
<i>Figure 19: The Password Model (Berthold, Spiekermann et al. 2005)</i>	<i>63</i>
<i>Figure 20: Visual Impression of User Scheme (left) and Agent Scheme (right)</i>	<i>64</i>
<i>Figure 21: UML Sequence Diagram: RFID tag – reader communication in a mall, User Scheme.....</i>	<i>64</i>
<i>Figure 22: UC Service Acceptance Model– Hypotheses and (expected directions).....</i>	<i>93</i>
<i>Figure 23: Scenario description of the ISA system displayed to study participants.....</i>	<i>94</i>
<i>Figure 24: UC-AM: relationships and path coefficients (fridge use [buy] / ISA / garage scenario)....</i>	<i>99</i>
<i>Figure 25: Two different potential man-machine function allocations for ISA</i>	<i>106</i>
<i>Figure 26: Control groups variation: Example of the adaptive desktop system.....</i>	<i>107</i>

Executive Summary

The current work begins by equating Ubiquitous Computing (UC) with the automation of everyday life. Drawing upon classical research literature on automation, we analyse UC, its application areas and classes, goals and challenges with a view to automation and thus untangle the mix of notions and definitions of the computing research area. Most importantly we describe how UC applications can be categorized alongside two dimensions of automation: the automation of information collection and analysis (input automation) and the automation of decision making and action (output automation).

Interestingly, 93% of all UC applications described in detail in the IEEE Pervasive Computing Magazine between 2002 and 2005 are dealing with input automation. UC technologies, thus, seem to allow us primarily to see things which were not accessible to us in the past, either because they were difficult to see or caused too much effort to observe. Moreover, the ability to see more or to be ubiquitously present is less focused on nature and the observation of infrastructures or objects (as is the case in classical automation).

Instead, UC technologies massively automate information collection about human beings: our own performances, states, whereabouts, social network activities, compatibilities to name a few. 2/3 of the applications investigated are focusing on these domains.

Against the background of this introductory analysis, Chapter 3 focuses on the input side of Ubiquitous Computing and, more specifically, looks into the benefits and challenges arising through RFID based information collection. We present an overview of the benefits inherent in the introduction of RFID item level tagging followed by a qualitative analysis of consumer concerns arising in this context.

An in-depth understanding of peoples' worries around the maintenance of their privacy in RFID enabled environments, as well as long existing insights into the psychology of control, leads to the deduction of three main system control requirements for RFID: First, RFID environments should be designed to provide people with cognitive control over when RFID read-outs occur. Second, decisional control is needed to determine when RFID based data collection is allowed to happen. And third, behavioural control in the sense of stopping tag-reader communication is required.

Against the background of this requirement analysis we present a snapshot analysis of 71 papers published on end-user privacy in RFID environments. We recognize however, that 80% of them do not live up to any of the control requirements identified. Consequently, we are led to propose a new privacy protection scheme (PET) for RFID tags: the User Scheme:

The User Scheme puts people into the position of the initiator of communication with RFID enabled environments seeing RFID chips 'locked' by default at retail store exits. Yet, claiming the User Scheme to be the PET solutions of choice would not be enough. An important part of this work is dedicated to the testing of the feasibility of the User Scheme. In particular we document the development of scales suited to measure the control people perceive over RFID infrastructures when they use the User PET and compare this performance with the control induced through a competitive PET which we denote as an 'Agent Scheme'. The result is that even though the User Scheme gives people more control over RFID information collection on a theoretical level, people have difficulties to accept any kind of complex PET. Instead more than 60% of over 500 study participants with which we test the different PET proposals empirically opt to kill RFID chips at store exits.

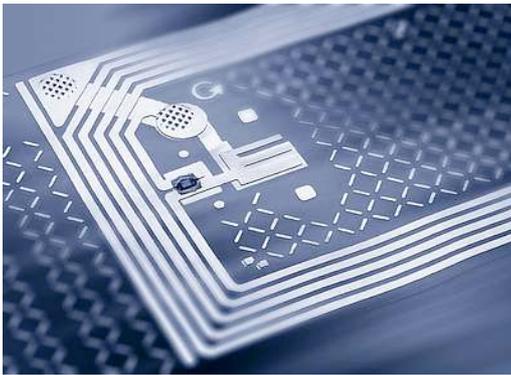
While Chapter 3 of this work is dedicated to the information collection side of Ubiquitous Computing, Chapter 4 adds another dimension to this work by investigating the effect of autonomous system action. Autonomous decision making or action selection through UC technologies is being investigated as to its acceptance by end-users. For this purpose we propose a novel UC Acceptance Model which investigates peoples' willingness to use or purchase UC systems based on a number of independent factors: most notably, their perceptions of control, of privacy maintenance, of risk and of usefulness inherent in a UC service.

Investigating these factors with approximately 4000 people, we prove the high relevancy of affective attitude for use and purchase intentions and its dependency on control perceptions. Interestingly the model also identifies privacy concerns as being much less important than expected by some UC

scholars. Across four UC scenarios, we propose and test the validity of the new acceptance model and find that it has a very high explanatory value to understand why people will accept or deny future UC services. We therefore believe that the UC Acceptance Model we propose is well suited to serve as a baseline model for acceptance research on UC in the future. Methodologically this work is one of those pioneering the approach of applying sound empirical analysis and testing to vaguely probable scenarios.

Preface

All writers owe a debt to their colleagues, friends, family and other supporters. I am no exception to this rule. This work would not exist without the kind support and intense co-operation of many colleagues and students, as well as the financial support of industry partners and political institutions. The following acknowledgements will serve to illustrate my gratitude.



In the fall of 2003 I began work on RFID with Oliver Berthold, Ph.D. candidate at the Institute of Computer Science at Humboldt University Berlin. His creativity and deep understanding of security technology led to the User Password Model to protect RFID chips (presented here in section 3.4) which we later patented in parts (Spiekermann and Berthold 2004; Berthold, Guenther et al. 2005; Berthold, Spiekermann et al. 2005)

He and Sebastian Zimmermann and I discussed this privacy protection scheme for RFID, its practical implications and pitfalls at great length and that inspired many of the control hypotheses discussed in this work and later tested empirically with users (presented here in section 3.6).

Likewise, the empirical user testing reported on in chapter 3.6 would not have been possible without the generous financial support of the Metro Group and their Future Store Team. The company sponsored the complex RFID privacy experiments with over 500 people over three years (2004-2006) and provided me with industry insights and thoughts all through this period. Most importantly, I needed to understand their perception of RFID as a value proposition to their customers. Some key results from this co-operation have already been published in the international magazine 'Communications of the ACM' (Guenther and Spiekermann 2005), the German journal 'WITSCHAFTSINFORMATIK' (Berthold, Guenther et al. 2005) and the technology assessment study I co-lead on Ubiquitous Computing for the German Ministry of Research and Education (Bizer, Günther et al. 2006).

While working on the control challenges inherent in RFID and peoples' fear of these, I realized that some industry bodies tend to play down the impact that RFID item level tagging could have on peoples' privacy and society at large. I therefore started to work with Holger Ziekow (Ph.D. candidate at the Institute of Information Systems at Humboldt University Berlin) to technically analyse consumer concerns formulated around RFID. In 2004 we jointly published a first version of the attack-tree analysis presented here in chapter 3.3. This analysis has been published both in a major IS conference (ECIS, (Spiekermann and Ziekow 2005)) and security journal (Journal of Information System Security, (Spiekermann and Ziekow 2006)) and was reprinted by consumer rights organizations to inform the public about RFID. We also used a longer and German version of the analysis to work with policy makers to demonstrate that consumer threats around RFID are for real (Spiekermann and Ziekow 2004).

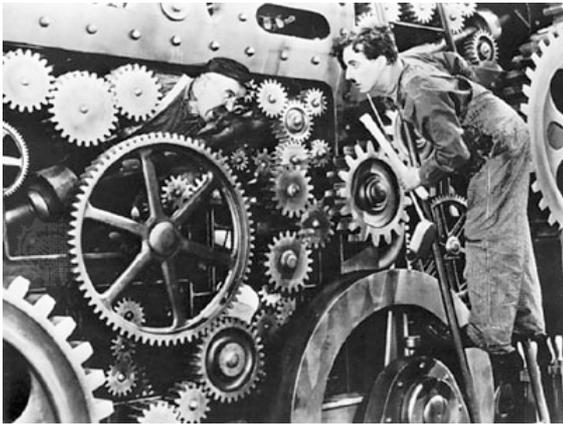
Recently, Sergei Evdokimov (Ph.D. candidate at the Institute of Information Systems at Humboldt University) and I delved into the huge pile of privacy technology literature that has been published on RFID between 2002 and 2007 (kindly supported by Elina Ivanova). We could confirm that the main privacy and security threads pursued by the RFID research community are pure cryptographic works on tag- reader communication. Even though these are valuable technical solutions to tackle, I argue that if UC engineers claim to want to address user control problems with RFID then it is not enough to only think about how to bring traditional crypto onto low resource chips (in sections 3.4 to 3.7). Instead, RFID and privacy engineers should think more of the actual control requirements people have

in different situations before they pop up with some technical protection schemes the aims and practicability of which are fuzzy and highly complex.

Generally I feel that in security research we often use a sledge-hammer to crack a nut. Instead of developing war-proof protection schemes for item-level RFID tags, we should invest more energy in the development of 'good-enough' security schemes which are usable. The User Scheme proposed by Oliver Berthold and myself could be an important step into this direction. Furthermore, the user studies presented here in chapter 3.2 make an effort to better understand and isolate user requirements. The control scales presented in chapter 3.4 should be used by privacy engineers to challenge their proposals with users.

Integrating all of these diverse analyses, models and empirical results into one chapter and adding many of the thoughts and reflections of these past years has been quite a challenge. Both Trevor Pierce (independent consultant on RFID) as well as Marc Langheinrich (assistant professor at ETH Zürich and major UC privacy expert) were very kind to give me very valuable and critical feedback here. Also the anonymous reviewers of the UbiComp'07 conference and Lorrie Faith Cranor helped me to optimize the RFID sections in this work, in particular the presentation of empirical RFID study results (Spiekermann 2007).

While information collection through RFID is certainly a major building block of this publication, it is not the only one.



Ubiquitous Computing engineers will also face a major problem with how to build smart devices in such a way that they do not deprive people of maintaining an upper hand. Mark Weiser once wrote that "the real problem [associated with UC] while often couched in terms of privacy is really one of control" (p. 694 in (Weiser, Gold et al. 1999). In another publication I have described the control problem associated with UC technologies as 'Technology Paternalism' (Spiekermann and Pallas 2005).

Together with Frank Pallas (Ph.D. candidate at the Institute at Computer Science & Society at the Technical University Berlin) and two thesis students (Hannah Krasnova and Ewa Baran), I explored the challenge I see when objects start to develop a life of their own. Hannah and Ewa confirmed this phenomenon with a group of international students at Humboldt University and documented their findings in a seminar paper (Krasnova and Baran 2005). Prof. Dr. Friedemann Mattern (Institute for Pervasive Computing, ETH Zürich, Switzerland) included an extended German version of the Technology Paternalism paper in his recent book on the 'Internet of Things' (Spiekermann and Pallas 2007).

Humans sometimes perceive machines or systems to develop a life of their own; it's an old science fiction theme (see for example the works of Isaac Asimov on robotics). However, it is also an issue discussed among scientists. Automation scholars refer to it under the terminus 'function allocation'. Prof. Dr. Hartmud Wandke from the Institute of Psychology at Humboldt University and a major expert in engineering psychology and ergonomics first pointed me to this stream of literature and later revised both the empirical work presented here on the UC Acceptance Model (in chapter 4) as well as a preliminary article on the parallels between automation and UC (which is part of chapter 2). I am most grateful for his thorough advice. But I also want to mention Prof. Friedemann Mattern and Prof. Lorenz Hilty (Head of the Technology and Society Laboratory at EMPA, St. Gallen, Switzerland) who both took many hours to revise my thinking about UC and automation.

Being an IS and management scholar by origin, I could not treat autonomous machine actions as a pure technical or pure psychological phenomenon. Also, I have not been interested to produce any

normative judgements on how UC technology should evolve. Instead I was (and I am) more interested in how consumer markets will most likely react to the new technological landscape created through UC and how UC should be technically designed in order to sell.

The willingness to purchase and use pro-active UC services are the dependent variables I am investigating here with the help of extensive empirical data collected from around 4000 Germans. Data collection would not have been possible to such an extent without the kind support of one of Germany's major newspapers called DIE ZEIT. Gunhild Lütge (editorial journalist at DIE ZEIT) strongly supported my efforts and gave me access to the newspaper's reader base for over a month in 2005. Both Dr. Guido Baier (assistant professor at the Institute of Psychology at Humboldt University) and Matthias Rothensee supported me in the set-up and analysis of the study leading to a first joint publication of the results (Baier, Rothensee et al. 2006). Matthias Rothensee in particular has been an outstanding peer to me over the past years. A Ph.D. candidate in psychology (at the Institute of Psychology at Humboldt University) he has been an excellent counterpart to jointly develop the hypothetical set-up of the UC Acceptance Model and assisted the statistical analysis.

I am grateful to the German Ministry of Research and Education (BMBF) which both financed the German Research Centre on Internet Economics (InterVal) and the Technology Assessment Study on Ubiquitous Computing (TAUCIS) both of which were crucial for funding and elaborating this research.

Finally and most importantly I want to express my gratefulness to Prof. Oliver Günther who has been my advisor since 2003 and has been coaching me in every respect over these past years, accompanying this work generously both intellectually and in terms of organizational backing.

1

Introduction

The historic development of computing can be broadly described by three historic waves: (1.) the ‘many persons, one computer’ era, (2.) the ‘one person, one computer’ era, and (3.) the ‘one person, many computers’ era.

The first wave (starting in the 1950s) is aptly termed the ‘many persons, one computer’ era. The one computer, coming in the form of a mainframe or minicomputer, was mostly used by specialists and deployed in industrial environments to reliably handle large scale data processing tasks.

The second wave of computing set in the late 1970s, the ‘one person, one computer’ era, is characterized by every employee or private person owning or using a computer, either for professional purposes or for leisure. By now, some industries (such as banking) see over 95% of their employees¹ working on computer terminals and 87% of German households² owned a PC in 2006. Thus, this second wave of computing is reaching saturation in recent years, at least in the industrialised part of the world.

The third wave of computing, which can be said to have started in the mid 1990s, is called the ‘one person, many computers’ era. It is characterized by computer chips increasingly being embedded in a vast array of consumer devices, such as smart phones, digital cameras, toys, cars, etc. The end-vision of this computing era is what some scholars have termed ‘Ubiquitous Computing’.

Ubiquitous Computing (hereafter often abbreviated as ‘UC’) refers to environments where most physical objects are enhanced with digital qualities. It is technically based on two building blocks: embedded computing and mobile communications (Lyytinen and Yoo 2002). Embedded computing implies that just about any kind of every day object, as well as the natural environment, human beings and animals, are infused with computing capabilities. Active and passive Radio Frequency Identification (RFID) tags, sensors, video cameras and the fusion of information stemming from these diverse systems are on the verge of leading to a ‘naturally’ computerized environment, while mobile wireless communication technologies such as RFID, Bluetooth or Wireless-LANs are used to hook up to these distributed computing devices and ‘capture and access’ information from them for aggregation, integration and service creation at the backend.

For all these technical building blocks of UC, strong scientific advancements and economic growth rates can be observed. For instance, by 2006 the semiconductor industry has grown into a \$ 248

¹ Statistisches Bundesamt (Deutschland): ‚IKT in Unternehmen - Nutzung von Informationstechnologie in Unternehmen, Ergebnisse für das Jahr 2006‘, published on 1.2.2007, Wiesbaden, 2007

² Statistisches Bundesamt (Deutschland): ‚Wirtschaftsrechnungen - Private Haushalte in der Informationsgesellschaft - Nutzung von Informations- und Kommunikationstechnologien (IKT)‘, published on 29.6.2007, Wiesbaden, 2007

billion worldwide business.³ Spending on RFID technology is expected to reach a worldwide level of \$ 8.1 billion by 2010.⁴ Mobile devices, in particular cell phones, now see a penetration of above 80% in industrialized nations such as Germany.⁵ And most nations are heavily investing in the build up of their mobile and satellite networks. These market developments support a current and apparently irresistible trend towards Ubiquitous Computing.

But: What does Ubiquitous Computing mean for people? For sure, the ubiquitous availability of computing resources is expected to strongly impact the professional work environment. A further increase of industrial automation is conceivable. Sensor networks will enable us to closely observe infrastructures. In manufacturing, as well as in logistics, myriad manual processes will be automatable through radio frequency identification (RFID) technology. Also, because of RFID and other localization technologies such as GPS, business, industry, and government will be able to seamlessly track and trace objects and people in real-time. Thus, a 'real-time economy' is a near-reality, thanks to UC.

However, people will not only be confronted with UC in their work places or industrial environments. They will find UC woven "into the fabric of everyday life" (p. 94 in (Weiser 1991)) with information services available everywhere. A new generation of ordinary objects will be enhanced through computing power. Chapter 2 of this work will give an extensive overview of what research laboratories are conceiving today. In fact, an analysis of 30 UC services presented in chapter 2 suggests that a majority of them will require private household investment or interact with people in a leisure context (see table 1). Consequently, UC products will, to a large extent, succumb the dynamics of mass market consumer goods.

These developments demand an answer to the question: what value will respective products offer its potential customers. Consumers will answer this question as they weigh the benefit against the cost of an item or service resulting either in market success or failure. The benefits of Ubiquitous Computing can to a large extent be characterized along the benefits of classical automation. On one side, UC allows to automate the acquisition and analysis of information. As the next chapter will show, 90% of UC services are enhancing our abilities to perceive the world around us. Seeing beyond our own physical space, monitoring others, infrastructures or our own internal states or behavior is a core benefit of UC. This 'information automation', which is called by some scholars also the 'informationization' of everyday life (in German: "Informatisierung des Alltags" (Mattern 2007)), is complemented by the view that UC will provide people not only with more information, but will also use it to pro-actively offer electronic services to people. Autonomous action execution as known from 'output automation' is the other, even more progressive, view on what Ubiquitous Computing is all about (Tennenhouse 2000; Ferscha 2007). Smart fridges deciding on our nutrition needs will replenish our food, cars will self-inspect themselves and schedule a meeting with the garage if required, phones will decide where to route a call so that it hits the recipient on the right spot, vineyards will maintain and water themselves as required for optimal yield - the list of services imagined to come is endless.

However, the history of innovation diffusion tells us that not everything which is invented will be taken up by people. In contrast, a majority of innovations fail, because they do not meet market demand. In Germany, for example, 67% of FMCG innovations (Fast Moving Consumer Goods) fail in their first year in the market and only 17% are successful from the beginning.⁶ For one thing, products and services often do not offer a 'relative advantage' to people to an extent that they are willing to invest in them. If they do, other inhibitors are playing a role for adoption as well: In particular, the

³ Semiconductor Industry Association (SCIA): "STATS: SICAS Capacity and Utilization Rates Q2 2007", sales volume publication, retrieved from: http://www.sia-online.org/pre_stat.cfm?ID=302 (August 14th, 2007)

⁴ The Economist, "Radio Silence", June 7th 2007

⁵ Statistisches Bundesamt (Deutschland): , Wirtschaftsrechnungen - Private Haushalte in der Informationsgesellschaft - Nutzung von Informations- und Kommunikationstechnologien (IKT)', erschienen am 29.6.2007, Wiesbaden, 2007

⁶ "Launches und Relaunches als Motor der Wertschöpfung. Was ist Top, was ist Flop?", Präsentation der GfK, GfK Consumer Scan Innovation Day, May 24th, 2006

complexity of a new product (its ease of use) is important for product acceptance as is its compatibility with established practices, social norms and user expectations (Rogers 2003).

We define acceptance in this work as the intention to buy and/or use a UC service. This does not mean that in this work we are going to predict the market take-up of UC services. But, the following chapters are written with the goal to identify key drivers for and potential impediments of UC service uptake. In chapter 3, we will look into consumer information services which are planned with the help of RFID technology and we investigate to what extent people accept and appreciate ubiquitous data collection through RFID. Complementing this information collection side of UC, chapter 4 investigates the drivers and impediments of pro-active UC services which aim to save people time. In both chapters we assume that engineers will have succeeded to overcome technical hurdles and will have been able to create seamless and easy to use UC services. Thus the 'complexity' issue often impeding an innovation's success is excluded from consideration here. What we are interested in, instead, is whether people see substantial benefits in the new service landscape, assuming that it works. And we want to find out how they weigh these benefits against the potential drawbacks of Ubiquitous Computing, in particular a loss of control.

The term control is mostly used in this work with a view to control psychology. Strictly speaking we are interested in control perceptions and how they can be influenced by technical designs. In chapter 3 we investigate peoples' perceived control over RFID based information collection. Uncontrolled automated information collection can seriously undermine peoples' privacy. Already (Weiser 1991), the founding father of UC noted that key among the social issues of UC would be the maintenance of privacy (p.102): "hundreds of computers in every room, all capable of sensing people near them and linked by high-speed networks, have the potential to make totalitarianism up to now seem like sheerest anarchy." We, therefore, build an important bridge in the work between privacy and control, viewing privacy primarily as a person's ability "to control access to the self or to one's group" (p. 24 in (Altman 1975). Yet, it is this very control which people could be deprived of in UC environments.

Based on qualitative research presented in chapter 3 we identify a loss of control as one major concern people have when they are confronted with RFID service scenarios. To address this concern we then delve into the technical options available to technically maintain control over RFID read-outs. Privacy enhancing technologies (PETs), which are proposed today by a growing research community, are scrutinized as to their ability to create a perception of control in people. For this purpose 540 experimental subjects have been confronted with film material documenting RFID service and control options available through current PET proposals. The relative importance of the perceived control induced through PETs is then investigated in comparison to the benefits people expect from RFID information services. It turns out that current PETs are not trusted by people. Consumers therefore seem rather to want to forgo the benefits of RFID and kill RFID chips than use complex PETs.

While chapter 3 deducts concrete challenges and acceptance issues surrounding RFID technology, isolates control issues surrounding the data collection process and derives requirements for privacy engineering, chapter 4 takes a much more inductive scientific approach. Chapter 4 focuses on the proactive service promise of UC and proposes a UC Acceptance Model (UC-AM) part of which is the dimension of user control over machine actions. Under the critical term 'Technology Paternalism' we already discussed, in earlier works (Spiekermann and Pallas 2005; Spiekermann and Pallas 2007), autonomous system actions as a major challenge for UC. Pro-active and autonomous decision making of machines has been questioned and investigated extensively in many areas of scientific research, in particular automation research (Wiener and Curry 1980; Endsley 1996; Sheridan 2000; Sheridan 2002) and software agent design (Maes and Wexelblat 1997; Jameson and Schwarzkopf 2002). However, investigations have mostly resided in the collection and documentation of design and interaction experiences with particular systems. No large-scale and theory driven empirical research with future users has been conducted on the issue to our current knowledge.

In chapter 4 we, therefore, propose the UC-AM where the perceived usefulness of autonomous UC services is weighed against their potential downsides, a loss of control and privacy. In doing so, we theoretically build not only on automation and agent research, but also on insights from technology acceptance research, psychology and marketing (Brehm 1966; Mehrabian and Russell 1974; Clee and Wicklund 1980). Finally, we look into how usefulness, control and privacy perceptions influence cognitive and affective attitude formation towards UC use.

The UC Acceptance Model is empirically tested with 3941 subjects who have given their view on four different UC scenarios. In two subsequent online and paper-based questioning sessions we are able to confirm that a difference in control allocation between humans and systems leads to different control perceptions followed again by negative emotions and a reduced willingness to buy and use a respective UC service.

In summary, this work will introduce the reader to Ubiquitous Computing and the new application landscape expectable from it (chapter 2). The conceptual proximity between UC and classical automation is going to be discussed (section 2.2), leading us to reason that UC can also be characterized as the automation of everyday life. In chapter 2 we lead the reader in a structured discussion as to whether such an automation is automatically a good thing. When it comes to the control of information collection (section 2.3.3), privacy appears as a major challenge for UC design. But also the automation of decision making and execution bears control challenges, which we discuss in section 2.3.4. Following this introductory part, the work has two relatively distinct foci. In chapter 3 we look at the information collection part of UC, focusing on RFID technology and investigate the abilities of privacy enhancing technologies (PETs) to induce a feeling of control in people over a ubiquitous reader infrastructure. In chapter 4 we look at the pro-active side of UC and theoretically build and test a general model of UC Acceptance applicable across technologies and services. Chapter 5 finally concludes with a summary of the findings and discussion of the contributions made to science through this work.

2

Ubiquitous Computing: The Automation of Everyday Life and the Role of Control

2.1 What is Ubiquitous Computing?

When Mark Weiser first used the term ‘Ubiquitous Computing’ in 1991, he described it as follows: “The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it [...] we are trying to conceive a new way of thinking about computers in the world, one that takes into account the natural human environment and allows the computers themselves to vanish into the background” (p.1 in (Weiser 1991)).

Since 1991 the idea of Ubiquitous Computing has inspired the computer science and engineering community, spurring many innovation domains which are essential pre-requisites for “getting the computer out of the way” (p. 76 in (Weiser 1993)). These include:

- a new breed of human-computer interface which is embedded in everyday objects, requiring little attention and supporting implicit interaction,
- services which are context sensitive and adaptive and have access to machine readable knowledge repositories from which they can derive ‘smart’ decisions , and
- communication technologies and service architectures which allow for continuous, seamless and ubiquitous availability of computer support.

In the first domain of innovations characterizing UC, computing is foreseen to be embedded in everyday objects and does not represent itself to humans in the form factor of a ‘computer’ any more. For this reason, scholars also talk about ‘hidden computing’, ‘calm computing’ (Weiser and Brown 1997), or the ‘invisible computer’ (Norman 1998). The notion of computers ‘disappearing’ is complemented by the idea that they are, however, ubiquitously present. Small sensors, RFID tags or receivers are planned to be part of a majority of objects. This is captured by the term ‘Pervasive Computing’ often used as a synonym for Ubiquitous Computing (Satyanarayanan 2002).

How does computing present itself to people. What is the new interface? (Lipp 2004) distinguishes ambient displays, tangible user interfaces and augmented reality as the three major categories of UC interfaces. (Schmidt 2000; Schmidt 2007) notes that UC is characterized by ‘implicit’ interaction. Implicit interaction means that sensor data, product IDs, location data, etc. will be interpreted by systems as input to trigger operations and that no direct and explicit input (such as text typing) is required. Major challenges to create such interfaces include the embedding of powerful computing resources into miniscule object structures, energizing them and networking them.

However, in order for Ubiquitous Computing to unfold its benefits, new interfaces are not enough. Once computing is available in objects it needs to be put to use in an intelligent and sensible way. Here, Ubiquitous Computing is referred to as ‘Ambient Intelligence’. Ambient Intelligence is a term chosen by the Information Society Technologies Advisory Group of the EU which subsumes that all major challenges of UC are resolved. It is presumed that UC services are context aware and adaptive (Coutaz, Crowley et al. 2005). Essential building blocks for context awareness are location technologies such as GPS and identity management for proper authentication and recognition, but also sensor fusion and activity recognition (Abowd and Mynatt 2000). In addition to context data, additional knowledge may be necessary for smart service delivery. However, much of today’s knowledge only exists in unstructured form. Knowledge discovery in unstructured information repositories (such as the Internet) as well as the evolvement of a semantic web may, therefore, be essential additional building blocks to support a computing that is not only ubiquitous, but also ‘intelligent’.

Finally, Ubiquitous Computing implies the seamless access to computing resources anytime and anywhere. In order to realize this, computing resources and services need to be ubiquitously accessible, interoperable and located where processing is most efficient. In order to realize this dimension of UC, distributed systems and advancements in the deployment of service oriented architectures as well as web services may play a role. Furthermore, the mobility of a user’s computing model must be enhanced (Lyytinen and Yoo 2002).

Within this vast landscape of technical issues and characteristics, the present work must, simplify and find an adequate frame of reference when referring to Ubiquitous Computing. For this purpose we want to broadly define Ubiquitous Computing as a vision of environments and people augmented with computational resources which provide information and services when and where desired (derived from (Weiser 1991; Abowd and Mynatt 2000)). Information and services are, however, not interesting in their own right. We must first determine what goals these UC technologies and services pursue. In what broad categories do they present themselves to people? What is the benefit of UC from the human perspective? And what are the challenges accompanying the envisioned computational landscape?

One might approach these questions by thinking of Ubiquitous Computing as the automation of everyday life. The next sections will show that the benefits, goals, challenges, pitfalls and classifications we have observed in the classical field of industrial automation over the past 100 years (and more) can, indeed, inform our thinking about UC environments. We will, therefore, show to what extent the two distinct research disciplines, automation and UC, overlap. Following this proof of conceptual similarity we then use some models and classifications elaborated in the automation research literature to conduct a structured analysis of UC. In particular, insights from control and function allocation research collected in the automation literature will be used to reflect on Ubiquitous Computing. Experimental work reported on in chapter 4 is furthermore based on models developed in automation research.

2.2 Ubiquitous Computing and the Automation of Everyday Life

2.2.1 Automation and Parallels to Ubiquitous Computing

“In the fullest contemporary sense of the term, automation refers to (a) the mechanization and integration of the sensing of environmental variables (by artificial sensors); (b) data processing and decision making (by computers); and (c) mechanical action (by motors or devices that apply forces on the environment) or “information action” by communication of processed information to people. It

can refer to open-loop operation on the environment or closed-loop control.” (p.9 in (Sheridan 2002)). Within this contemporary definition of automation (which is also visualized in figure 1) it becomes clear that automation has outgrown its original meaning of the mechanization of manual tasks (19th century view of automation) and goes beyond the notion of the (closed) loop and mechanical control cycle (20th century view of automation). Instead, automated systems are increasingly characterized by the leverage of computing power which fuels their increasingly complex logical core.

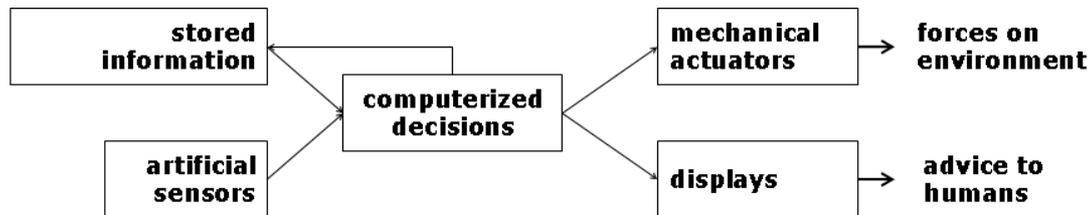


Figure 1: The scope of automation (p.10 in (Sheridan 2002))

When we look at figure 1, the similarity between Ubiquitous Computing and automation becomes apparent: Information explicitly given to a system is stored and complemented by data implicitly collected via sensors. The combined input is aggregated and analysed to then, either trigger physical reactions onto the environment, or provide humans with enhanced information. Those UC scholars who promote the ‘pro-active’ mission of UC (Tennenhouse 2000) echo the notion of triggering forces that act on the environment in an automated way. Others put relatively more emphasis on the enhanced information provision of humans to assist them in better decision making. They describe Ubiquitous Computing “as the prospect of connecting the remaining things in the world to the Internet, in order to provide information on anything, anytime, anywhere” (p.3 in (Mattern 2001)). We will discuss below whether one or the other (in essence complementary) perspective on the deliverables of UC is more prominent. But, in any case, the lines of thought reflect that UC has the same output as classical automation: pro-active automated action as well as information display.

Scholars from both research streams, automation engineering and Ubiquitous Computing could of course argue that figure 1 lacks the human element. Human interaction (Schmidt 2000; Schmidt 2007) is seen as a core of UC while automation is related almost exclusively to object actions. Stored information and in particular sensor data thus relates to ‘things’ not people when it comes to automation. Even though this is true, the term ‘Internet of Things’ -often used interchangeably to talk about Ubiquitous Computing, - denotes the fact that UC equally equips mostly objects with computing. Thus, even though UC scholars think in terms of human interaction they are dealing with the enhancement of objects and physical infrastructure, just as automation does.

In another argument against the symbiosis of automation and UC, some commentators say that in automation ‘forces’ are used to impact on the physical environment. Thinking about many UC applications such as interactive toys, ambient displays, tracking devices, etc. such direct forces are not foreseen as part of many UC services. However, one could argue that while automation applies direct forces, UC applies indirect forces. Thus, automation induces, for example, a machine unit to physically stir in one direction. An interactive toy would simply not respond to a particular ‘false’ movement or emit a sound which forces people to engage in corrective action. In an indirect way UC applications, therefore, also induce changes to physical processes.

A third argument distinguishing UC and automation says that Ubiquitous Computing does not only use sensor data as input, but also leverages other technologies’ data such as RFID-tag IDs or location data. Here it must be noted that with the advent of precise localization technologies, industry also increasingly takes advantage of these in industrial automation. Classical automation is not reduced to ‘artificial sensors’ any more as figure1 falsely suggests. As an example one can think of GPS based automated container loadings in big harbours.

Finally, the field of automation has not actively claimed the ambition to be invisible, hidden or calm while UC scholars like to put this vision at the forefront of their thinking. Still, many modern automated systems such as automobiles or cockpits are incarnations of invisible computing. Automation engineers have succeeded to create many calm and hidden applications successfully in use today.

To conclude, automated systems and ubiquitous computing systems share a significant common core of how they work. Against this background, insights from automation literature will be used in the next sections as a guiding structural frame to discuss the emerging field of Ubiquitous Computing, its goals, challenges and control issues.

2.2.2 Classifying Ubiquitous Computing Applications

2.2.2.1 Classifications used to characterize automation

Literature suggests three main classes of automation (Wickens 1992; Scerbo 1996) which are relating to the reasons for having automation. These are widely identical with those of Ubiquitous Computing: First, automation is used when it comes to performing functions which are beyond human ability. Second, automation comes into play with tasks humans are poor at doing. And third, it is exploited for activities undesirable for humans to pursue.

Originally, these classes of automation were formulated with a view to physical processes (e.g. automating repetitive physical tasks at assembly lines). However, as supervised processes get more and more complex, information processes required to inform computerized decisions are in themselves being automated. We find an example in the collection of distributed sensor information for aggregation and display in plane cockpits. (Parasuraman and Sheridan 2000) therefore make a distinction between input and output automation (see figure 2). The automation of input functions refers to the acquisition of sensory information and the aggregation and interpretation of this information to an extent not feasible for human operators. In contrast, the automation of output functions refers to decision making, action selection and execution of a system based on the information collected. The latter is the more classical conception most people have when using the term “automation”. (Parasuraman and Sheridan 2000) write: “automation may also be applied to input functions, i.e., to functions which precede decision making and action” (p. 287).

In the remainder of this work we use this distinction between input and output automation in order to structure our analyses. UC applications are categorized in the next section as being either input- or output related. And empirical investigations presented in chapter 3 and 4 differentially focus on input or output automation through UC respectively.

When it comes to the goals of automation, the study of the role of assistance systems is useful. Assistance systems have been investigated as part of automation theory. They are the human interface with automation and reside on automatically collected and aggregated information put at the disposition of human operators. They can equally assist in triggering and monitoring output automation. (Wandke 2005) distinguishes six goals of assistance systems: The first goal is to enhance our perceptions (1). Display assistance helps us to render the invisible visible, to amplify signals, create redundant signals or transform dispersed or unrecognizable signals into something we can perceive. The second goal of automation assistance is to help us interpret data (2). Interpretation can reside in labelling assistance, amplification of information as well as explanation assistance. A further level of assistance can be reached when assistance systems do not only help us see and interpret things, but also motivate us (3) and give us feedback (4). Motivation can come in the form of activation and warning assistance as well as coaching assistance. Feedback assistance is aggregated information to help us recapitulate events to potentially improve behaviour or conditions. Finally, assistance systems can prepare decision making presenting us solely with final choices to take (5). At the highest level of automation they would execute autonomously and eventually inform us about activities (6).

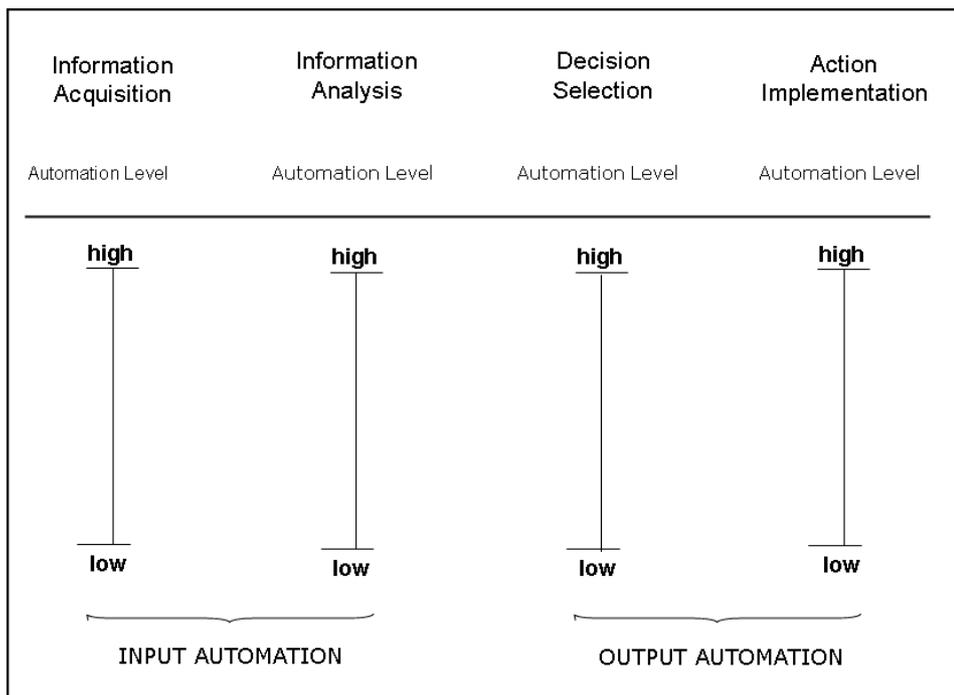


Figure 2: Four stages of automation with distinct automation levels

2.2.2.2 An overview of Ubiquitous Computing applications

In order to categorize UC applications and better understand their goals from a user perspective we conducted an analysis of UC applications described in the IEEE Pervasive Computing Magazine. As a basis of analysis, we chose three years of articles in twelve issues of the IEEE Pervasive Computing Magazine dating from 2003 to 2005 as a snapshot. We included an article in the analysis if it is dedicated to the description of one project only and includes a detailed description of the services delivered to users. The “new product” section of the magazine presenting products already out in the market was excluded from the analysis. Equally, exemplary applications, projects mentioned shortly as scenarios and robotics were not considered.

As a result of this choice only 28 articles out of the 174 published in the respective period could be included in the analysis. In these 28 articles, 30 UC applications have been described. Table 1 summarizes and characterizes these applications. Its columns 2 to 4 contain the three classes of automation described above. And columns 5 to 10 characterize each UC application according to the goals it pursues. Only those goals of automation have been considered which are explicitly referred to by the authors and architects of the respective solution. In addition to these characterizing elements of the analysis, we also looked into whether the most likely party to fund the infrastructure would be a professional or private entity and whether people would most likely be in contact with the application in a leisure or professional context. Appendix 1 contains a description of all 30 services summarized in table 1.

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

	Project/Application Name	Goals of UC Applications									most likely investor	use context W=Work L=Leisure
		Classes of Automation			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	Gustbowl	x			x						priv.	L
7	UNSEEN		x		x						prof.	W
8	Vineyard Computing		x		x	x				x	prof.	W
9	iCAMS	x			x	x		x			priv.	L/W
10	CareMedia	x			x	x	x				prof.	W
11	CyberCrumbs		x		x						prof.	W
12	SHARP – Project – CareNet Display	x			x			x			priv.	L
13	SIMBAD	x			x		x				priv.	L/W
14	CodeBlue	x			x						prof.	W
15	Robot and Sensor Networks	x			x		x				prof.	W
16	SHARP – Activites of Daily Living (eADL)		x		x	x					prof.	W
17	Self Healing Minefields (APPS)		x	x	x					x	prof.	W
18	SHARP – Project		x		x		x				priv.	W/L
19	Personal Server-CareLog	x			x						prof.	W/L
20	Serendipity-Introductions	x				x	x				priv.	L
21	Context Phone - ContextLogger	x			x	x					priv.	L
22	Context Phone - ContextContacts	x			x	x					priv.	L
23	ContextMedia - Aware		x		x						priv.	L
24	Mobile Service Toolkit - Virtual Queuing			x	x					x	prof.	L
25	Mobile Service Toolkit - Interactive Ads			x	x					x	prof.	L
26	CamShell – SHGCheckbook			x		x				x	prof.	L/W
27	IM4Sports (=Interactive Music for Sports)	x			x	x	x			x	priv.	L
28	FIPM (Football Interaction Process Model)		x		x	x	x				prof.	L
29	SKI		x		x	x	x				prof.	L
30	SensorHogu		x		x		x				priv.	L

Interestingly, we found from table 1 that 93% of the UC applications presented from 2003 to 2005 are including or exclusively focus on the automation of information collection and interpretation. This means that they allow us to recognize more than we would physically be able to and partially use this information to motivate us, give us feedback, or prepare and execute decisions. 40% (12) of the 30 UC applications have no other goal than this pure collection of information or automation of data input and display. 12 out of the 30 (43%) applications allow for seeing things totally inaccessible to us in the past ('can't do'-class of automation). For example, the Gustbowl project allows for sharing presence information via two interlinked bowls placed in two households. Symbolic placement of objects (such as keys) in the bowl are then representing activities (such as homecoming) (Keller, van der Hoog et al. 2004).

The opportunity to gain inaccessible or additional information is complemented by services which allow for viewing things at which humans are naturally poor at observing ('do poorly'-class of automation). This is the case when it comes to the monitoring of states of activities, of changes concerning the human body or the environment over a longer period of time, or by combining

multiple information sources. 12 out of 30 (40%) UC applications presented are of this nature. For example, two projects, GTWeb and Aware, describe the possibility to automatically documenting peoples' movements and events over time and across spaces so that others can see and track what their peers are doing or where they are (Spinellis 2003; Raento, Oulasvirta et al. 2005). In the past, this type of functionality would probably have been realized by paper-based diaries which one could share with others physically. The Argus project employs technology which allows for the observation of sandbars, ocean intensity and wave breaking in nearshore areas (Holman, John et al. 2003). Such observations were previously made by guards walking the shores (see figure 5).

Much fewer UC applications are in the realm of output automation in the sense that decisions are prepared or executed automatically and proactively by systems. In fact, only 9 out of 30 applications (30%) include some output automation. Eight out of these (26%) integrate some execution function, mostly supporting activities which people don't like doing. For example, a restaurant PDA saves waiters continuous walks to the counter when ordering foods (Stanford 2003). Also self healing landmines (Merrill, Girod et al. 2004) which can be switched off remotely serve as another example. Only 2 out of the 30 applications analyzed (7%), however, can really be called pro-active in the sense that the computerized environment takes a decision for the human and presents him with the results. These are the Vineyard Computing and the Interactive Music application for sports (Burrell, Brooke et al. 2004; Wijnalda, Pauws et al. 2005).

This summary of UC applications shows that, for the time being, the pro-active vision of UC is still far from being the reality of prototypes presented up to 2006. Instead ubiquitously seeing and perceiving more than we ever did before about people, things, and events seems to be at the forefront of current application design.

2.3 User Acceptance of Automation and the Role of Control

The remainder of this work will deal with both input automation (chapter 3) and output automation (chapter 4). In two very distinct parts, in terms of methodology and level of analysis, we will discuss the acceptance and control challenges which arise for the two sides and stages of automation.

Beyond the classification of UC classes and goals, table 1 shows that unlike institutional environments (where automation generates economies of scale) many UC services are requiring private household investment. 40% of the investigated UC services envisioned by the IEEE scholars require that individuals will spend money on them. An additional 20% need to be sufficiently appreciated by consumers in their leisure time in order to justify institutional investment. Consequently, UC services need to be designed for user acceptance. For this reason, user acceptance is the dependent variable investigated at the core of this work.

User acceptance is often measured by government agencies as a general tendency among citizens to view innovations (Renn and Zwick 1997). However, we define acceptance here as consumers' concrete intentions to use or buy, approach or avoid the technology in concrete scenarios. We therefore have a much narrower focus. In chapter 3 acceptance of implicit data collection is being investigated. In chapter 4 the acceptance of pro-actives UC services is being analysed. In both parts the relative importance of perceived control is carved out as a determinant factor for UC acceptance. Before delving into these relatively detailed and specific analyses, however, we first want to give an overview of current knowledge on user acceptance of UC and the role of control therein.

2.3.1 Concept and Study of User Acceptance

The construct of user acceptance has been investigated at different levels of detail depending on the scientific community in which it has been discussed. At the most generic level it has been studied in the innovation diffusion literature (Rogers 2003). Here, acceptance is mirrored in the term ‘adoption’ and is investigated over longer periods of time. Often, the units of observation embrace more than just one technology and deal with the take-up of whole new practices. At a more granular level, and looking into the concrete adoption of individual information systems, the IS discipline has been analysing adoption under the term ‘technology acceptance’.

A so called ‘Technology Acceptance Model’ (TAM) has evolved (Davis 1989; Davis, Bagozzi et al. 1989; Venkatesh and Davis 2000; Venkatesh, Morris et al. 2003; Davis and Venkatesh 2004) which sees acceptance reflected in peoples’ intentions to use or buy systems. Using and buying, however, is again determined by a level of acceptance bound to individual system characteristics. This is where the field of Human-Computer Interaction (HCI) as well as ergonomics set in. Here, ‘system acceptability’ is primarily viewed as ‘practical acceptability’. And to reach practical acceptability, usability is the most important factor. Usability testing is looking into the learnability of a system, its efficiency, the degree to which it satisfies users, its memorability and finally its ability to minimize user errors (Nielsen 1993). When new systems are built alongside a ‘Human Centric Systems Development Life Cycle’ usability testing is a regular part of the analysis, design and implementation phase in order to ensure system acceptance (Te'eni, Carey et al. 2007).

Designing Ubiquitous Computing applications systematically ‘from the human out’ and applying usability testing rigorously could probably become a hygiene factor for UC acceptance. Already today, first evaluation frameworks are being proposed to tackle this issue in UC (Scholtz and Consolvo 2004). However, the application of HCI methodology typically requires a prototype at the outset of investigations. Consequently, the results of this kind of acceptance research are typically limited to one particular system. The insights gained cannot readily be generalized across systems. Furthermore, prototype based acceptance research is often retrospective in nature since systems must be advanced enough in their engineering before they can be tested with users. As a result, some researchers have been calling for complementary research approaches that would be required to understand UC adoption patterns. (Lyytinen, Yoo et al. 2004) observe: “Whereas current research focuses mostly on field observations and reflections on live experience, the domain of ubiquitous computing is amenable for futuristic, visionary research that is prospective and prescriptive in nature. Topics addressed should be prospective rather than retrospective – they should be of concern to our action now and its trajectory for the future” (p. 709).

Against this background, we tackle the issue of acceptance more in line with IS researchers. We investigate peoples’ pre-purchase intentions to use and buy UC services when they are confronted with UC scenarios. Furthermore, we analyse attitude formation on future systems. In chapter 4 we hypothesize that cognitive and affective attitudes are impacted by usefulness, risk, privacy and control perceptions and that they will be moderating system acceptance in a hierarchy of effects. If people emotionally embrace UC environments (have a positive affective attitude) then they will probably also plan to buy and use them. And, in contrast, if they develop a negative emotional or cognitive evaluation they may try to avoid them. Emotional response to UC systems is, therefore, an important variable in the hypothetical model on UC acceptance we propose below. It draws from recent reflections of Donald Norman on the “Emotional Design” of products (Norman 2004) and Bagozzi’s view on the importance of emotion in marketing (Bagozzi, Gopinath et al. 1999). Both authors would support the thinking that emotional design could be a key when it comes to the acceptance of the automation of everyday life. Not surprisingly, ‘consumer appreciation’ has been one of the first dependent variables used to investigate the acceptability of autonomous UC home products (Rijsdijk and Hultink 2003).

2.3.2 Meaning of the Term 'Control'

2.3.2.1 Perceived control

Humans' emotions and behavior are strongly determined by the degree of control they have over their environments. In the 1970s (Mehrabian and Russell 1974) found that perceived dominance over an environment – equated to control in the psychological literature (Bagozzi, Gopinath et al. 1999) - would lead people to approach it. In contrast, when people are deprived of control, they avoid environments (Mehrabian and Russell 1974), show reactance (Brehm 1966), feel helpless (Seligman 1975; Abramson, Seligman et al. 1978), are unhappy (Thompson and Spacapan 1991) and even die earlier (Langer and Rodin 1976).⁷ Perceived control “refers to the extent to which an agent can intentionally produce desired outcomes and prevent undesired ones. When individuals believe they can do this, they are said to have personal control, perceived control, or a sense of control” (p. 554 in (Skinner 1996)). Perceived control is the conviction that “one can determine the sequence and consequences of a specific event or experience” (p. 385 in (Zimbardo and Gerrig 1996)).

Perceived control has found an entry into the study of information systems when it comes to the motivation to use them. (Novak, Hoffman et al. 2000), for example, found that perceived control over the use of E-Commerce websites is a major determinant to experience flow which again determines the depth of interaction. HCI has embraced control through feedback as one of the most accepted guidelines in the design of interaction (see figure 3 from p. 211 in (Te'eni, Carey et al. 2007)).

-
- Feedback should correspond to a user's goals and intentions.
 - Feedback should help evaluate a user's goal accomplishment.
 - Feedback should be sufficiently specific to control user activity.
 - Feedback should help develop accurate mental models of the system.
 - Feedback should fit the task representaiton (verbal and visual).
 - Feedback should fit the type of behavior (controlled, automatic).
-

Figure 3: Design rules for feedback to promote control

Even though subjectively perceived control is believed by many psychology theorists as the more powerful predictor of functioning than the control actually exercised (Averill 1973; Langer 1975; Burger 1989), some control perceptions still depend on whether an event is in fact 'controllable'.⁸ The degree to which people perceive controllability has often been related to personality in the psychological literature.⁹ Beyond individual differences in perceiving control, however, judgements of

⁷ Irving Janis wrote: “When a person notices that protective actions are having little observable effect in bringing an end to an extremely disagreeable experience, his or her initial reaction is usually an upsurge of anger and protest. If the person's efforts to regain a sense of control continue to be thwarted, he or she is likely to become demoralized. After that happens, the person copes less effectively and ultimately develops profound feeling of helplessness and depression. These extreme reactions, which are usually accompanied by apathy and social withdrawal, are pertinent to both mental health and physical health. There is a growing body of evidence that the malignant emotional sequence associated with loss of perceived control...not only increases subjective suffering but also impedes physical recovery and sometimes leads to untimely death. Fortunately, however, there is also evidence that the malignant sequence can be prevented or interrupted by...interventions that enable distressed people to see themselves as having sufficient control over what happens to them to cope successfully” (p. 10 in Langer, E. (1983). *The Psychology of Control*. Beverly Hills, USA, Sage Publications.)

⁸ It should be noted that some people also suffer from illusions of control Langer, E. (1975). "The Illusion of Control." *Journal of Personality and Social Psychology* 32(2): 311-328.

⁹ One personality variable often cited is the 'locus of control' of a person. This is a person's tendency to attribute the causes of events either to her own actions (internal locus of control) or to some

actual controllability are important for peoples' behavioural reactions. According to (Averill 1973) three types of control can be distinguished: (1) cognitive control, which is a person's possibility to understand and interpret a threatening event, (2) behavioural control, which is the possibility to take direct action on the environment in order to influence threatening events, and (3) decisional control, which is the opportunity to choose an action among possible options. This conceptualization of control is particularly valuable when trying to bridge the gap of what it means to design a system that is perceived by its users as controllable.

2.3.2.2 Control systems

At this point it should be noted that from an engineering perspective the controllability of a system has nothing to do with perceptions. The words "control, controls or controllability", when used in an engineering context, are typically related to control theory and control systems. Scientifically rooted in cybernetics (Wiener 1948), control theory states that a control variable (e.g. temperature or pressure) is chosen to influence a system so that the system attains a desired optimal state. Controllability in this sense means whether controls are available so that a system will reach its optimal state in finite time. Control theory is a field of applied mathematics underlying control systems which again are intimately linked to the concept of automation (Encyclopaedia Britannica Micropedia 2005). A control system is a "means by which a variable quantity or set of variable quantities is made to conform to a prescribed norm" (p. 589 in (Encyclopaedia Britannica Micropedia 2005)). Control systems are coming in the form of closed-loop and open-loop systems depending on whether they are inherently self-sustaining.

Closed-loop systems are at the core of automation. They are inherently self-sustaining and self-directed and as such do not require human intervention to operate. Increasingly, feedback (and feedforward) controls are integrated in automated systems, and their interplay has become more complex. Since the 1950s multiple-loop systems are spreading. Here, system feedback is initiated at more than one point in a process, and corrections are made at more than one point. This adds to the complexity of automation which can increasingly only be handled by computers. Therefore, a distinction is being made today between 'modern control' and the older and simpler 'classic control' (Encyclopaedia Britannica Micropedia 2005).

2.3.2.3 Supervisory control over automated systems and UC applications

In industrial manufacturing environments, transportation (aviation, rail systems, automotive and spacecraft), health care and teleoperations where automation has been heavily deployed, insights have been gained on how humans interact with automated systems. In 1988 (Sheridan 1988) first described the human role in automated environments as the one of a supervisor and proposed a model of 'supervisory control'. The framework, broadly depicted in figure 4a, represents humans as operators who supervise processes through several layers of computing (Sheridan 1988). At the lowest level processes and their states are observed by sensors. The information collected can, in some cases, be used directly to trigger low-level control loops leading to self-sustained and controlled processes. In other cases, the information is forwarded to "task-interactive" computers which are typically located close to the equipment they are monitoring. These task-interactive computers serve as integrators and aggregators of information about the diverse low-level processes taking place. Relevant information is then passed on to the human-computer interface which also serves as the command-control device for

external forces, such as fate (external locus of control) Rotter, J. B. (1954). Social learning and clinical psychology. Englewood Cliffs, Prentice Hall.

humans. Increasingly the human-interactive computer is a more sophisticated assistance system confronting humans with more or less control alternatives. Humans are left with two supervising roles in this model: One requires them to monitor and process the information which is being presented to them by the computer (i = information). The other requires them to intervene in the process (c = control) where it is not driven by the assistance system.

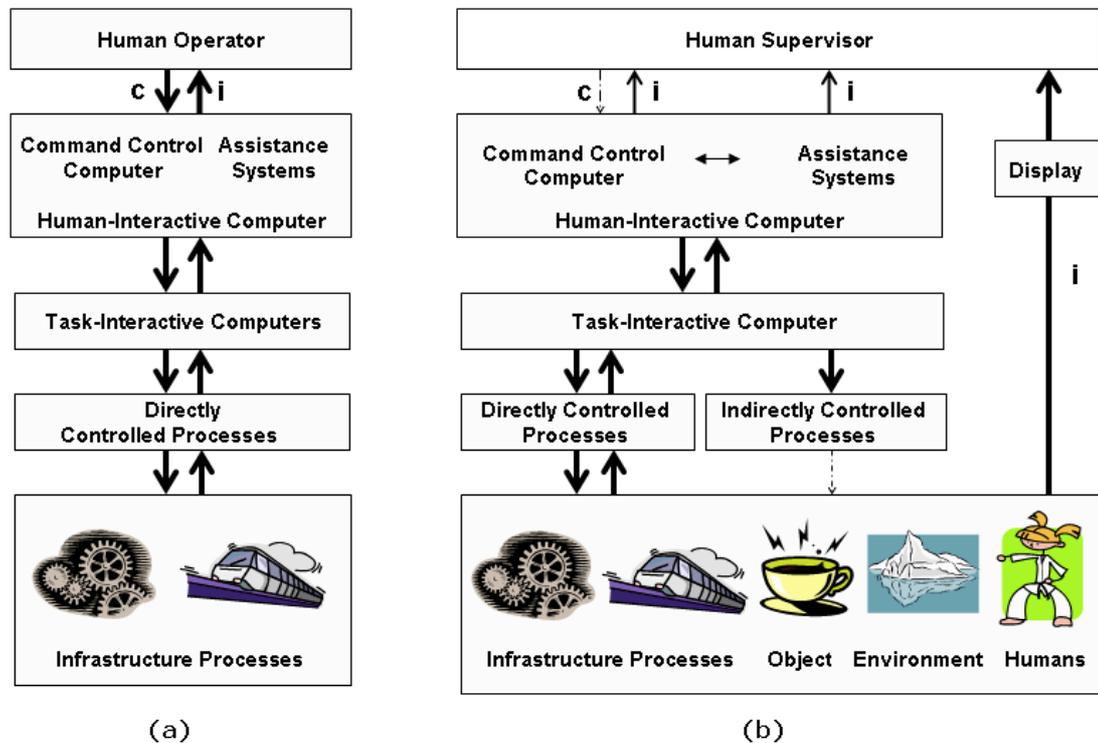


Figure 4: Model of supervisory control in classical automation (a) and adaptation to UC (b)

As figure 4b shows, UC applications can be described by a similar assembly. For example, read-outs from passive RFID chips are filtered according to pre-established rules by a reader infrastructure. In a logistics process readers in a distribution centre will access product deliveries reading out and filtering products' Electronic Product Code embedded in the RFID chip. The information is passed on to a middleware (analogue to a task interactive computer) which integrates the data collected according to pre-determined rules. Middleware filters may use information about expected deliveries to decide whether the captured list of incoming goods is complete. For complete deliveries it may automatically file the process as completed and save the information in a billing system for later handling (analogue to Sheridan's self-controlled processes). For incomplete deliveries it may pass on a warning note to the respective web interface of an Enterprise Resource Planning System (which is the human interactive computer). Here, the human operator may take over process handling. The information flow from the objects observed to the human operator in typical UC environments is thus well captured by Sheridan's model. Equally, self healing landmines (Merrill, Girod et al. 2004) and robot networks (Kumar, Rus et al. 2004) included in table 1 could be directly described by figure 4a.

However, some important distinctions, which are captured in figure 4 b and which are related to the aspect of control, exist between UC applications and classical automation. For one thing, human operators in Ubiquitous Computing are even more becoming passive observers than they are in classical automation, because 40% of UC applications focus exclusively on the automation of information input, but do not offer any means to intervene in the underlying process. The reason for this lack of intervention opportunity – or “control function” in Sheridan's speak - is primarily that the object of observation is different from that in machine automation. In UC environments the objects of observation are typically other human beings (2/3 of the cases analysed) or nature (13%) (see table 2

below). Both of these are hardly integrable in a mechanized direct control process. In addition, even if objects or infrastructure are enhanced with computing resources they often only include passive computing elements such as passive RFID chips or sensors which are able to transmit information about an object, but do not allow for a backchannel to the object. This is captured in figure 4b by describing humans as supervisors rather than operators. Humans' diminished control options are visualized in figure 4b by a very thin c-arrow. If action is taken by an operator or a task interactive computer, it often triggers a third system which indirectly influences the underlying force. For example, a vineyard may be watered by a watering system separate from the infrastructure collecting information about the vineyard's state (Burrell, Brooke et al. 2004). Process control is therefore illustrated in figure 4b as two separate entities influencing the underlying forces (directly or indirectly).

The model of supervisory control shows that the hierarchy of processes depicted for automation are transferable to those of UC. Consequently, similar challenges and questions arise. For example, how much control do people want? How many functions should be delegated to the lower levels of computing? How can it be ensured that human supervisors are not becoming too alienated from physical processes? One UC scholar wrote that "getting humans out of the loop and into supervisory and policy-making roles is a necessity for systems with faster-than-human response time" (p. 48 in (Tennenhouse 2000)). Looking at figure 4 though this thinking appears hardly generalisable for UC. At the very right of figure 4b it becomes apparent that UC will allow automating the observation of human beings. Will the observed not want to be in the loop? The next section on control over automatic information collection will delve into this question in more detail.

At the left side of figure 4b, UC processes and those of classical automation largely overlap. Here, classical debates led in automation are probably transferable to UC. Automation scholars have been investigating optimal man-machine function allocation and have for long asked how much control people should maintain over automated processes. They hold some answers to the question which has recently reached the UC domain: "Is automation automatically a good thing?", (p. 56 in (Derrett 2006)). Parallels and insights gained here will be systematically discussed in the next two sections.

2.3.3 Acceptance Challenges of Input Automation and the Role of Control

2.3.3.1 Privacy or control over automated information acquisition

For the analysis of UC applications the distinction of different automation goals is useful, because it shows that 28 of the 30 applications investigated (93%) are related to input automation. 26 help humans to perceive things or acquire information hardly available to them in the past (86%). 12 out of 30 (40%) go a step further and aggregate or interpret the information acquired.

The benefits derived from these input services (as well as subsequent storage and availability of the data) are probably substantial. They include, for example:

- the collection of real-time information about the physical state of the elderly that cannot be cared for personally (Consolvo, Peter Roessler et al. 2004; Sixsmith and Johnson 2004),
- the gaining of new insights into our own physical states and ways to improve (Michahelles and Schiele 2005; Wijnalda, Pauws et al. 2005),
- the possibility to see others who are far off (Shi, Xie et al. 2003),
- the ability to be present beyond one's own physical space (Keller, van der Hoog et al. 2004)
- as well as the means to document one's life and share precious moments with peers (Spinellis 2003; Raento, Oulasvirta et al. 2005).

This short list of benefits shows that only just the automatic and ubiquitous capture of (and access to) information allows for the creation of consumer services which human kind has for long admired in fiction. One only has to take a step back and think of the witches' crystal ball which allows seeing remote others unnoticed and from a distance.

Equally, myriad magical artefacts described in novels such as Harry Potter are representations of what can be done with the UC technologies presented (Rowling 2003). For example, ancient picture frames described in the Harry Potter novels are used to share presence (just as in the SMART classroom application (Shi, Xie et al. 2003)), the Marauder's Map is used to track others sorcerers' location in Hogwards castle (just as the GTWeb (Spinellis 2003) or the MagicMap¹⁰ application) or wizard Dumbledore's 'Pensieve' allows recapitulating precise happenings of the past (as described in the Personal Server project (Hayes and Truong 2005)). This short analogy makes plain that UC technologies bear the promise of capabilities we have long desired for. Consequently, a proliferation of consumer markets driven by consumer appreciation and acceptance does not seem far fetched.

Beyond such potentials of the technologies for consumer markets, UC's information acquisition capabilities bear major industry opportunities. Automatic tracking and tracing of goods, fraud and counterflight detection, fled management, teleworking all these are examples of how UC technologies can impact the economy. The 'real-time economy'- we can expect it to be realized through Ubiquitous Computing. Consequently, its information collection capabilities are here to stay.

However, despite these benefits, the ubiquitous automatization of information collection also bears challenges. One such challenge concerns a potential over-reliance on automated information collection. The other resides in privacy problems created through these collection practices.

Through the delegation of control over information collection to a technical infrastructure, a potential over-reliance on the information collected may ensue, a "misuse" as some scholars have termed this inherent challenge of automation (Parasuraman and Riley 1997). Over-reliance could lead to a decreased ability or skill to observe things ourselves in the long run, a 'degradation of skills' (Endsley 1996). It could lead to an over trust in the knowledge produced by machines in comparison to what humans observe. And, the fact that everything is observed may as well lead to a reduction in real attention.¹¹ As Langer showed, humans easily make "premature cognitive commitments" if they believe that something is reliable (Langer 1989). People may make the commitment to always rely on the availability of machines leading to a questionable degree of dependency on the technical infrastructure.

Most importantly, however, UC presents the potential to undermine privacy through ubiquitous data collection. Table 2 enumerates the extent to which privacy could become an issue in UC enabled environments. Column 4 in table 2 looks into whose activities are being supervised by the system. Entities observed could be human beings, objects or the natural environment. In some cases a human being is supervised via an object he or she uses. In this case, column 4 specifies the human as the object of supervision, not the mediating object. One need also ask whether the one being supervised is also the recipient of the information (column 5). In some cases the supervised person (SP) is identical with the supervisor (S) (annotated as SP = S). In other cases the supervised person is not identical with the supervisor (SP ≠ S). In again other cases, the information collected could be put at the disposition of both, the person supervised as well as a third party (for example, a person coached and the coach) (=≠).

Table 2 shows (in column 4) that over 2/3 of the UC applications presented in the IEEE Pervasive Computing Magazine between 2003 and 2005 put human beings at the forefront of observation. We do not seek so much to observe objects or nature as much as to observe, through UC capabilities, each other. And in 90% of these human focused applications (see column 5) the observer is not necessarily identical with the observed. In 50% of human centred applications people get feedback about or insights into their own behavior or states. In the other half of the cases, 3rd parties are observing them.

¹⁰ <http://www2.informatik.hu-berlin.de/rok/MagicMap/index.htm>

¹¹ For example, detecting falls of an elderly person as described by the SIMBAD system is a valuable application, but what happens if relatives rely too much on the system, replacing it partly for personal care and by this happen to disregard a fall undetected by the system?

Automating information collection about each other seems a perverse idea at first sight. (Lahlou, Langheinrich et al. 2005) characterize the information collection process in UC as a new dimension of privacy threat due to the unprecedented collection coverage foreseen, coupled with the invisibility of the collection process, the amount of potentially intimate data collected, and the system interconnectivity planned. (Boyle 2003) reflects on the necessity to manage the 'attention of the Ubicomp environment'. Repeatedly George Orwell's science fiction novel '1984' about a modern society is cited by UC critics. The author described, for example, the following scenario: „The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it, moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment” (p. 6 in (Orwell 1949)).

Orwell's dystopia shocks readers because the book's characters can not change the settings of the ubiquitous telescreens. Had people been given control over them, enabled to switch them on or off as needed, the fiction would have lost a lot of its impressive horror. After all, control determines privacy. Privacy, the way it is defined, does not mean that one should never be watched by others or that information collection should be forbidden or anonymous, per se.

As was outlined above, Altman (Altman 1975), one of the main sociological privacy scholars in the Western world, views privacy as “the selective control of access to the self or to one's group” (p. 24). Other scholars share this view. (Schoeman 1984) describes privacy as the control an individual has over information about himself or herself. And (Margulis 2003) reflected on several decades of privacy research when writing: “Privacy, as a whole or in part, represents control over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or minimize vulnerability” (p. 245).

Table 2: Objects of supervision and supervisor relationships in UC applications

	Project/Application name	Goals of UC application		Object of Supervision	Supervisor Relationship
		input automation		O = Object	SP = S → =
		see/ perceive	interpret	H=Human	SP ≠ S → ≠
		1	2	3	4
			E=Environment		
1	Restaurant PDA Pads (APP)			O	-
2	Smart Classroom	x		H	≠
3	GT Web	x		H	≠/=
4	Argus (APP)	x	x	E	-
5	Vocera Communicator Badge System			O	-
6	Gustbowl	x		H	≠
7	UNSEEN	x	x	E	-
8	Vineyard Computing	x	x	E	-
9	iCAMS	x	x	H	≠
10	CareMedia	x	x	H	≠
11	CyberCrumbs	x		H	≠
12	SHARP – Project – CareNet Display	x	x	H	≠
13	SIMBAD	x		H	≠
14	CodeBlue	x	x	H	≠
15	Robot and Sensor Networks	x	x	E/O	-
16	SHARP – Activities of Daily Living (eADL)	x	x	H	≠
17	Self Healing Minefields (APPS)			O	-
18	SHARP – Project	x		H	≠/=
19	Personal Server-CareLog	x		H	≠/=
20	Serendipity-Introductions	x	x	H	=
21	Context Phone - ContextLogger	x	x	H	≠/=
22	Context Phone - ContextContacts	x		H	≠
23	ContextMedia - Aware	x		H	≠/=
24	Mobile Service Toolkit - Virtual Queuing	x		O	-
25	Mobile Service Toolkit - Interactive Ads	x		O	-
26	CamShell – SHGCheckbook		x	O	-
27	IM4Sports (=Interactive Music for Sports)	x	x	H	=
28	FIPM (Football Interaction Process Model)	x	x	H	≠/=
29	SKI	x	x	H	≠/=
30	SensorHogu	x	x	H	≠/=

Control over input automation and thus maintenance of privacy has evolved as a major research area with a goal of giving people the possibility to decide what, when, where and by whom information collection is taking place (Ackerman, Cranor et al. 1999; Adams and Sasse 1999; Adams 2000; Annacker, Spiekermann et al. 2001; Acquisti and Grossklags 2005; Garfinkel and Rosenberg 2005). Some first insights into peoples' privacy preferences in UC have been gained. Investigations in mobile location services have shown, for example, that agreeing to be found and identified through location tracking services depends on the inquirer of the information and on the individual's context (Lederer, Mankoff et al. 2003). Privacy management platforms which give people control over when, where and by whom they can be located have therefore been propagated and enforced by major mobile operators (Vodafone 2003).

At the same time, Privacy Enhancing Technologies (PETs) are developed for almost all areas of technology where automatized information collection about people is taking place. For example from E-Commerce we find software solutions for anonymously surfing the Internet (Berthold, Federrath et al. 2001), for inhibiting transaction tracking (Oliver Berthold and Federrath 2003), for managing multiple personal identities (Camenisch, Shelat et al. 2005) or for taking informed decisions about whom to trust and whom to avoid (Cranor, Guduru et al. 2006).¹² Also in those technical areas forming the core of UC services, such as location services and embedded systems, an active research community has emerged which, from an engineering perspective, works on technical solutions to maintain control over UC environments.¹³ Here, researchers work, for example, on how to facilitate the management of privacy preferences (Myles, Friday et al. 2003), to technically enforce controlled release of location data (Schulzrinne, Tschofenig et al. 2007), to anonymize tracking data (Stajano 2003), to ensure proper authentication (Pering, Sundar et al. 2003), to embed privacy policies in services (Friedman, Smith et al. 2006) and to come up with new privacy management interfaces (Streitz, Röcker et al. 2005; Cornwell, Fette et al. 2007). Scientific work on how to design the controls in UC so that people perceive control is therefore under way. Chapter 3 below will extensively discuss the work of the research community focusing in particular on privacy solutions for RFID technology and contribute to its current state of knowledge.

2.3.3.2 Privacy or control over automated information analysis

Table 1 classifies a number of UC services as allowing for more than just information collection. A service is classified in table 1 as containing some analysis or interpretation if not raw data is simply transmitted to enhance our perceptions, but is instead enriched and augmented so that we can grasp the information in an enriched way. An example may clarify this difference: in the Smart Classroom and Gustbowl projects (Shi, Xie et al. 2003; Keller, van der Hoog et al. 2004), UC technology allows one to see or perceive the action of others, but this perception is a plane transmission of a state of being. In other applications, this plane information is enhanced with extra information. For example, in the SKI project and in the Argus projects (Holman, John et al. 2003; Michahelles and Schiele 2005), video data is not plainly transmitted, but pictures taken are enhanced with an interpretation of what is seen (see figure 5 taken from p. 18 in (Holman, John et al. 2003)). In other applications such as iCAMS (Nakanishi, Takahashi et al. 2004) multiple context information about a callee is aggregated to prioritize where to best contact him or her.

Such automated analysis may be highly useful because "humans have been proven again and again to be poor monitors of occasional or slowly changing signals" [p. 209 in (Sheridan 2000)]. They are apt to fatigue and seek distraction. They are also limited in simultaneously integrating a multitude of information into their decision making (Bettman, Johnson et al. 1990). Some UC applications could

¹² A good source of advancements made in this research community can be inspected by following the PET workshop (Privacy Enhancing Technologies): <http://petworkshop.org/2007/>

¹³ A good insight into the activities can be gained from papers published in the privacy workshop series organized at the Ubicomp conferences in 2002 ("Socially-Informed Design of Privacy-Enhancing Solutions in Ubiquitous Computing"), 2003 ("Ubicomp communities: Privacy as boundary negotiation"), 2004 (Ubicomp Privacy: Current status and future directions) and 2007 (UbiComp Privacy: Technologies, Users, and Policy)

therefore help societies to increase their safety by watching nature and critical infrastructure more closely than this was possible before.



Figure 5: Argus Project: Video based analysis of near shore environments

Automized information analysis concerning people creates the challenge of a potential ‘disembodiment and disassociation’ (Bellotti and Sellen 1993). When video data is collected, combined and augmented, it may suggest something about people and their interactions which isn’t true. Some people may have been filmed the very moment they were yawning which suggested that they were sleepy during a workshop session while in reality they were not (Adams and Sasse 1999). The same risk applies to sensor information which may transmit information about the physical fitness of an individual which may not represent the perceived truth for that person. As aggregation of sensor information is typically based on probabilities and heuristics, the apparent “truth” coming as a selected, emphasized or augmented piece of information out of the system may not always be the real truth.

The question is, therefore, how people can control or influence the process of information analysis and aggregation. In one approach people are given direct access to those technological infrastructures that channel some of the analysis and aggregation made. For example with location middleware platforms users are given access to specify their privacy preferences (Myles, Friday et al. 2003). Also, we may indirectly increase control over information use, its aggregation and analysis if we increase the accountability of those who analyse and aggregate data (Nissenbaum 1994). Concrete approaches on how this could be realized practically are, however, missing.

In another control issue related to information analysis we must be concerned with how people will be characterized based on their data. Early privacy research in the Internet and offline context has shown that people are concerned about ‘reduced judgements’ that could be made about them (Smith, Milberg et al. 1996). This fear is aggravated by the fact that ubiquitous data collection could, if information flows are not controlled (Lange, Nonnengart et al. 2002), also lead to a combination of data from multiple sources. “A piece of information here or there is not very telling. But when combined together, bits and pieces of data begin to form a portrait of a person” (p.20 in (Solove 2006)). As the section 3.2 below on RFID technology will show, such profile creation seems to be a practice feared and criticized by consumers. This gives rise to the question of how to give people physical control over information once it is out. Unfortunately, few technical answers exist in this domain The art of forgetting would be ‘a useful void in the age of Ubiquitous Computing’ as (Mayer-Schönberger 2007) notes.

2.3.4 Acceptance Challenges of Output Automation and the Role of Control

Figure 1 and table 1 show that output automation can reside in two types of services: (1) the display of information that contains some advice for humans, and (2) systems that use their input information to autonomously pre-select decisions and, eventually, execute. The need to control any of these activities has very different dynamics in different scientific disciplines. While control over information display has been researched in learning (Klayman 1988) and attention psychology (McFarlane 1999; McFarlane 2002), and recently also in marketing (Ariely 2000), decision and execution control is a subject traditionally treated in the automation literature (Sheridan 1988; Parasuraman and Sheridan 2000) as well as in software engineering (Maes and Wexelblat 1997; Jameson and Schwarzkopf 2002).

2.3.4.1 Control over the information flow and interrupts

When information is displayed to users in UC environments they could potentially exercise control over what should be presented, when, where and how. Table 1 gives a number of examples of applications which provide users with information, either in order to give them feedback or to motivate them to act in a certain way. For example, the SHARP project presents an application which triggers activity based reminders such as taking medications (Philipose, Fishkin et al. 2004). Serendipity is an application motivating people to get in touch by sending them mutual invitations if their personal interest profiles match (Eagle 2004). (Wandke 2005) would refer to this kind of applications as activation, coach or warning assistance.

Against the background of these applications we must ask when to best interrupt users to provide them with the respective information and how much control to give people over this point of interruption as well as the interrupt itself. Extensive research in notification platforms (software engineering) and in automation literature has treated this question (McFarlane 1999; McFarlane 2002; Horvitz, Kadie et al. 2003). Here it was found that if people are given control over when to handle an interrupt (so called 'negotiated interruption') their quality and efficiency in fulfilling a primary task as well as timeliness and overall performance are increasing (McFarlane 1999; McFarlane 2002).

Having control over the information flow of a site can help consumers to better match their preferences, have better memory and knowledge about the domain they are examining (Klayman 1988), and be more confident in their judgments (Ariely 2000). This is especially true in an E-Commerce context where one goal is to increase the 'stickiness' of a page and thus motivate users to stay on. (Novak, Hoffman et al. 2000) showed that perceived control over the interaction enhances the probability that users experience flow and thus stay longer online.

For UC applications these research findings suggest that if businesses want to gain user acceptance they might (1) give people control over when they receive information and are free to handle it at a time of their choice and (2) give people some control over the way advice is derived. For example, setting up the SHARP application (which gives people activity based reminders (Philipose, Fishkin et al. 2004)) could involve users to specify upfront which activities and activity patterns are chosen to trigger notifications. The drawback of such a user involvement is an increase in transaction processing and set-up cost for users.

2.3.4.2 Decision and execution control

Industrial automation has witnessed a multitude of control issues. For instance, pilots in cockpits most frequently ask the questions: "what is it doing?", "why is it doing that?", "what will it do next?" and "how did it ever get into that mode?" (Woods 1996). The reason for these questions is that people often lack situation awareness (Endsley 1996). They do not recapitulate quickly enough in what mode a machine is in, sometimes they have forgotten about underlying mechanisms at work (Endsley

1996), or poor system design has led to a discrepancy between the “designer’s conceptual model” and the “user’s mental model” (Norman 1988; Scerbo 1996). By 1994 a review of commercial aviation accidents had shown that 88% for those with human error involved a problem with situation awareness (Endsley 1996). An interesting case presented in the IEEE magazine stems from the project iCAMs where engineers had to de-automate their application due to this very problem of users’ lack of situation awareness (Nakanishi, Takahashi et al. 2004). When testing the iCAM system the researchers noted, that “some users were puzzled by instances in which a caller intended to contact the callee but a callee’s colleague answered the call. This phenomenon resulted from the redirection destinations consisting of personal cellular phones and common telephones in homes or offices, and the caller not knowing where the message would be redirected in the automatic routing. As a result, the callers tended to feel slightly uneasy” (p. 82-83 in (Nakanishi, Takahashi et al. 2004) In cases such as this one, systems may have a ‘perceived animacy’ from the user perspective. “When a device is complex, has high autonomy and authority, and provides weak feedback about its activities it can create the image of an animate agent capable of independent perception and wilful action.” (p.7 in (Woods 1996)).

Due to this control challenge and also in order to maintain human autonomy vis-à-vis machines, automation researchers have been looking into the degree to which machines should automatically execute functions or just prepare function execution through the assistance of the decision making process (Fitts 1951; Kantowitz and Sorkin 1987; Parasuraman and Mouloua 1996; Sheridan 2000). Optimal function allocation is at the core of “human-centred automation” (Billings 1991). Human-centred automation theory has produced a number of approaches which can serve as guidelines for optimal function allocation. One, Fitt’s MABA-MABA list (Fitts 1951), suggests to allocate tasks to humans and machines in accordance to their relative strengths and weaknesses. Fitt’s list suggest that humans are better than machines in detecting small amounts of visual, auditory or chemical energy, at perceiving patterns of light or sound, at improvising and using flexible procedures, at storing information for long periods of time, and recalling appropriate parts, at reasoning inductively and exercising judgement. Machines are, in contrast, better at responding quickly to control signals, applying great force smoothly and precisely, storing information briefly and erasing it completely and reasoning deductively. However, these man-machine trade-offs are also moving targets as machine capabilities progress and human capability can be enhanced through training and practice. Consequently, no clear guidelines on how functions should generally be shared between humans and machines have yet evolved leading to Sheridan’s provocative article, “Function Allocation: algorithm, alchemy or apostasy? (Sheridan 2000). To understand at least allocation options, Sheridan has formulated a model where he depicted eight to ten design alternatives on how control can be shared between humans and machines (Sheridan 1988; Sheridan 2002). These levels range from one extreme, where a computer does everything and where people have no control, to the opposite extreme where individuals do not involve machines (full control). Table 3 summarizes this control scale and it equally demonstrates how it can be applied to two exemplary interactive UC services scenarios investigated in a later section of this work (chapter 4).

Some insights into peoples’ willingness to delegate decisions to machines have been gained in the context of software agent research. Despite economists’ hope that agents could solve the problem of asymmetric information in markets and give people powerful support in making better purchase decisions (West, Ariely et al. 1999), experimental research has shown that shopping agents to which product choices are delegated often fail to motivate users to finally accept the agent’s decision (Häuble and Trifts 2000; Spiekermann 2004; Diehl 2005; Spiekermann, Strobel et al. 2005). People prefer to take purchase decisions only after extensive manual search regardless of agent advice (Spiekermann 2001; Spiekermann, Strobel et al. 2005). In an automation context (Lee and Moray 1992) show that only when subjects realize that their manual strategy does not work they switch their strategy and integrate automation.

Software engineers working on the design of software agents have accumulated some experience on how to improve users’ perceived control over agents (Maes and Wexelblat 1997; Jameson and Schwarzkopf 2002). They mention, for example, that agents should include meaningful dialogue with users, provide reasons for suggestions, always give short-cuts to ‘pause’ and ‘resume’ agent activity, only gradually advance to take over decisions for humans, and respect that people have very different pre-dispositions of how much control they generally desire (Maes and Wexelblat 1997).

Table 3: Exemplary application of automation levels to two UC scenarios

	8-Stages of Automation and Control (Sheridan 2002)	Intelligent Fridge 	Speed Limit 
1	C offers no assistance; the H must do a task completely herself.	H must do the shopping, The fridge only chills the food.	H breaks manually when seeing a speed-limit sign.
2	Upon request C shows all alternative options to do a task H executes.	H requests list of items to be repurchased. H then repurchases any items she deems necessary.	Upon request C offers warning support for speed limit control. H considers advice.
3	C recommends specific way to do a task. H has to execute or not execute recommendation.	C recommends items to be purchased and proposes repurchase which H can approve.	C recommends a certain speed. H can follow advice or not.
4	C recommends specific way to do a task. Executes upon H approval.	C asks H, and if he approves purchases the shopping list.	C asks H to apply braking force, and applies it upon approval.
5	C recommends specific way. Allows H a restricted time to veto before automatic execution.	C buys the shopping list if for some time there has been no veto from H.	C waits x seconds after the street-sign signaling before braking autonomously.
6	C executes automatically, and informs H about action taken.	C buys the items from the shopping list and informs H.	C decelerates, and reports the act to H.
7	C executes automatically and informs H only if asked to.	C buys the items from the shopping list and reports list upon request.	C decelerates, and reports to H if requested.
8	C selects the method and executes task. H is out of the loop.	C does the entire re-purchase, without report to H.	Automatic brake mode, no manual braking possible.

H = Human, C = Computer/Machine/Object

While such insights on control design are highly valuable for UC system engineers, they must also decide, when considering the degree of automation, the goal of a service. Is it the best joint man-machine system performance in terms of efficiency and productivity? Or, do human satisfaction, work motivation, and emotional well-being take the lead over efficiency? In classical automation environments which are of professional nature, productivity, efficiency and safety have been at the forefront of thinking leading to an increased delegation of control to machines (Wiener and Curry 1980). Yet, for UC services this could in many cases be different. Often people even “feel stress due to subjectively unpredictable behavior of technical systems” (p 863 in (Hilty, Som et al. 2004)). As was outlined above 60% of UC applications are for use in peoples’ leisure time. Consequently, the optimization equation for function allocation may be apt to different dynamics than the one in traditional automation. Here, the cognitive and affective reaction of consumers to a product or service will largely determine a UC service’s success in the market.

2.3.5 Conclusion: Is Automation Automatically a Good Thing?

Ubiquitous Computing is often characterized as ‘smart’ and ‘intelligent’. Calm computing services, operating almost as human servants in the background, serve us with information and attendance whenever and wherever we need them. And, indeed, the long list of benefits of the UC systems discussed in this chapter explain the unclouded efforts undertaken in a worldwide computer science community to realize the visions first described by Mark Weiser in 1991. However, if UC is described in a much plainer and almost disillusioning way as the automation of everyday life, we must all ask if, as UC scholars have asked, ‘automation is automatically a good thing’ (Derrett 2006).

Automation at its core seeks to relieve humans from complex or physically demanding tasks. Historically (and in particular in the industrial revolution) it has been primarily related to the physical task environment. In the information age, we have started to embrace the potentials of ‘information automation’ (Parasuraman and Sheridan 2000). Video systems, sensors, satellite systems, RFID reader infrastructures and mobile networks allow us to automate the capability to see. 86% of the UC applications presented in the IEEE Pervasive Computing Magazine between 2003 and 2005 are inherently about this very ability. In many cases the information is then aggregated, pre-processed and used as input for better decision making or for triggering reactions to what has been observed. Assistance systems serve as the interface to automation and give us access to complex pre-processed information for decision making or take decisions for us pro-actively. (Wandke 2005) depicts this enhancement of people through automation as shown in figure 6. Viewed from this perspective, automation is certainly a good thing.

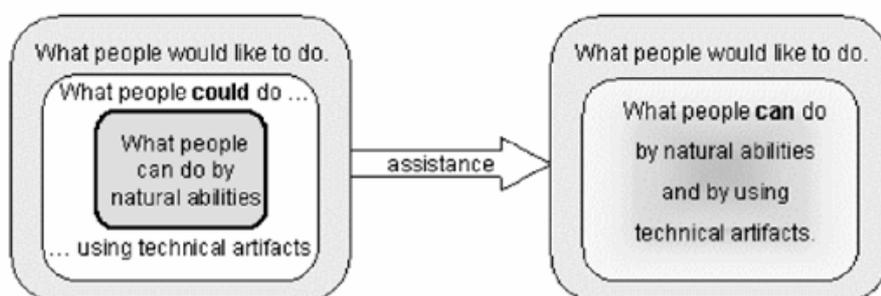


Figure 6: The goal of automation

However, as this chapter has shown, the enhancements for UC cannot be considered thoroughly beneficial without restraints. The structured analysis of UC alongside its inherent goals has shown that uncontrolled and uncontrollable automation bear ethical challenges and threaten well-being. This becomes obvious when looking at the downsides of automatic information collection and analysis (the input side of UC): Even though we can gain a richness and completeness of information never accessible before, the maintenance of privacy or “the selective control of access to the self or one’s group” (p.24 in (Altman 1975)) is a social as well as a technical challenge. In order to maintain privacy in UC environments, people need to be informed about where, when and by whom they are accessed. They need to be able to control information collection about themselves in order to exercise their personal right to informational self-determination.¹⁴ Automation of information collection is, therefore, a promising, but at the same time, ethically challenging step. The next chapter of this work

¹⁴ In Germany’s constitutional law informational self-determination is indirectly covered, because it is considered by jurisdiction as a general personal right.

will extensively focus on this very issue. It will carve out the precise privacy and control requirements people have vis-à-vis one particular UC technology - RFID - and it will delve into how controls could be designed in order for people to 'perceive control' over the automation of information collection.

When input automation is discussed, the automatic analysis and interpretation of data collected must also be discussed. Especially when it comes to the simultaneous processing of many information points and the inference of patterns from large data pools. Yet, in section 2.3.3.2 we also showed that this process creates the challenge of disembodiment and disassociation (Bellotti and Sellen 1993) as well as peoples' fear to be apt to a reduced judgement (Smith, Milberg et al. 1996). An over-reliance on automated pre-processing of information could lead people to trust machines more than their own observations and intuitions. Such a 'decision-bias' in favour of systems, but also the failure to analyse information personally, can in some cases lead to false decisions. When we ask whether automation is automatically a good thing, therefore, we have a double-edged sword: On one side, automation of information analysis is a good thing if it can provide us with insights we would not be able to deduce ourselves and which are highly reliable and smart enough to consciously avoid reduced judgements. On the other side, its excessive use may also be questioned. First, Fitt's list suggests that humans are better at exercising judgements than machines (Fitts 1951) and judgement is a core of interpreting information. And second, the less people are involved in information analysis and aggregation the less they will be skilled at it and would start to "internally automate", as Sheridan puts it (p.457 in (Sheridan 1996)).

Finally, UC allows for output automation, for autonomous decision making or 'pro-active' services as well as decision preparation. Although pro-activity is one major vision for UC, very few applications observed really live up to this expectation (not even 10%). In the automation literature it has been observed that delegating too much control to machines can lead to problems of situation awareness which, again, are the source of errors. Furthermore, people resist the introduction of automation. Strong debates between airlines and pilots as to the degree of automation in cockpits has forcefully demonstrated this and Europeans still resist electronic gearshift. Both pilots and drivers resist the automation of what they regard to be their own tasks. The psychology of control would argue that this is because perceived control over events is essential for well-being and that a deprivation of control leads to feelings of helplessness and an avoidance of environments. In professional environments it has been observed, of course, that people in their employment setting are adjusting to the level of control they are given. In some countries automatic gearshift is also very well accepted (e.g. in the US). However, an interesting question is whether UC services offering to automate everyday life, will be so welcome by consumers that they will really generate sufficient market demand. As the analysis of table 1 has shown, 60% of UC services aim to facilitate peoples' private lives. Consequently, many UC services can be regarded as consumer goods. Chapter 4 of this work will therefore delve into the question of whether subtle differences in the allocation of functions are actually perceived by people and whether more or less perceived control will lead to more or less willingness to purchase UC services. Equally, we will investigate what effects perceived control has on the cognitive and affective evaluation of a UC service and the subsequent intention to use it. If allocation of control has a significant impact on intentions to buy and use UC services, then UC engineers will need to put considerable efforts into this particular characteristic of their technical designs. Whether automation is a good thing is then going to be decided by consumer markets.

3

User Concerns, Technical Challenges and Control Options over Automated Information Collection – The Case of RFID

While chapter 1 and 2 have given an introduction to Ubiquitous Computing and familiarized the reader with the general distinction of input and output automation, this chapter is focusing exclusively on the former. More precisely, it looks into the automation of information collection with the help of RFID. Table 1 has shown that 86% of UC applications integrate automated information collection. Diverse technologies are used for this purpose. These include video systems, sensor networks, mobile as well as satellite networks. One major technological enabler of automatic information collection about people and objects is Radio Frequency Identification (short RFID).

3.1 Introduction to RFID

RFID is considered to be an important technological building block of Ubiquitous Computing, because it is the major enabling technology for the ‘embeddedness-dimension’ of UC. Embeddedness is realized through RFID by integrating RFID chips into just about any kind of everyday object. These tiny chips can currently become as small as 0.3 millimetres square.¹⁵ Joint with a thin film antenna, these components form a tag that can either be attached to an object or directly integrated into a label, the packaging or fabric of an item. Mobile or stationary ‘readers’ are then used to retrieve or encode the chips’ information and enable further computing services. To do so they do not need a line of sight to an object and can be placed – depending on the radio frequency spectrum used – at various distances from the object (see table 4).

Even though RFID is a relatively old technical concept (used already since the mid 1940s), the technology has strongly gained in relevance since the US department of defence showed its potential for supply chain control, and EAN and UCC came together and decided in 2001 to develop it as a compatible standard for reading next generation UCC and EAN barcodes. EPCglobal was created as a joint venture between EAN and UCC, the two global barcode

¹⁵ RFID Journal, March 14th, 2003, Hitachi unveils smallest RFID chip, retrieved on July 19th, 2007 from: <http://www.rfidjournal.com/article/articleview/337/1/1/>

standardization bodies, in order to focus upon RFID. EPCglobal currently represents around 1100 companies from diverse industries and, in particular, the consumer goods and retail sector. EAN and UCC merged in 2004 to form GS1. Since barcodes are attached to virtually all products (and even product subcomponents) RFID tag manufacturers have had a large incentive over past years to bring down the price of item level tags to below 5 Euro cents. The early 1990s vision of computer scientists to ubiquitously embed computing power into virtually all everyday products has gained a highly realistic dimension through item level RFID tagging.

Table 4: RFID frequency bands and read ranges

	LF	HF	UHF	Microwave
<i>Frequency Range</i>	< 135 KHz	10 ... 13.56 MHz	860 ... 960 MHz	2.4 ... 5.8 GHz
<i>Read Range</i>	~10 cm	~1 m	2 ~ 5 m	~100 m
<i>Coupling</i>	Magnetic, Electric	Magnetic, Electric	Electromagnetic	Electromagnetic

taken from (p. 26, (van Lieshout, Grossi et al. 2007)

3.1.1 The Many Forms of RFID

RFID technology comes in many different forms. Much of the technology to date has been built to serve the needs of closed proprietary systems with specific use cases. Consequently a highly diverse industry has evolved over the past 70 years providing its components. When one reflects on information collection through RFID, one sees an important distinction between active and passive RFID tags. Active RFID tags contain a proper energy source (i.e. a battery). These tags can self-initiate the sending of their data over a longer distance (e.g. up to 100 meters for 2.4 to 5.8 GHz tags). Passive RFID tags, in contrast, do not have a proper energy source, but are instead powered by a reader. Passive tags can thus only respond to reader requests and - depending on the frequency – can send their information over a few metres distance.

In addition to this distinction between active and passive RFID tags, a further distinction is made between different tag classes. Generally, tag classes range from 0 to 4 discerned upon tags' memory, power source and other features (EPCglobal 2005). Each class has more capability than the one below it and is backwards compatible. Originally, Class 1 tags were considered passive Write Once Read Many (WORM) tags with minimum memory to hold only an EPC number. Class 2 tags are passive field programmable tags with extended user memory and authenticated access control. Class 3 tags have an integrated power source and sensing circuitry. And Class 4 tags are active tags, allow for tag-to-tag communication and ad hoc networking (EPCglobal 2005). GS1's division EPCglobal which develops RFID standards proposed EPC Class 1/Generation 2 tags (EPCglobal 2003; EPCglobal Inc. 2005). These tags are of passive nature and their numbering scheme is foreseen by GS1 to replace the existing barcode on pallets and cases as well as items. The frequency band used is the UHF band between 860 and 960 MHz. This implies that they have a legal¹⁶ read range of two to five metres (some industry experts also report on six to eight metres).

¹⁶ „Legal read range“ in this context refers to the assumption that only authorized readers access the tag by powering it with 2 (EU) to 4 (US) Watt. Potentially, unauthorized readers could achieve longer

Due to the distinct capabilities of different RFID standards, this report necessarily focuses on one particular type of RFID for the analysis presented hereafter. More precisely we are concentrating on passive EPC Class 1/Generation 2 tags as they have been specified by EPCglobal. The focus is justified against the background that this class of tag will potentially become the de-facto standard in many industries for item-level tagging. A recent study among German industry players revealed that the majority of tags are expected to be of passive nature (65% of system integrators expect this, 83% of those from an industry background, 72% of service providers, an 45% in retail). The frequency band of 860-960 MHz is favoured by 40-54% of the study participants (Pater and Seidl 2007).

3.1.2 Information Infrastructures and Architectures for RFID

EPC Class 1/Generation 2 tags which foresee little data to be directly stored in an object's chip. Instead, each chip is programmed with an 'Electronic Product Code' (EPC) (EPCglobal 2003). This EPC is used as an identifier to find information about the object to which it is attached on the Internet. The information available on the Internet is created and maintained by myriad parties involved in an object's lifecycle from the moment of its assembly (manufacturer) and distribution (logistics service provider) to its sale (retailer), use (consumer) and recycling. The parties involved are supposed to store relevant information they collect about an object and then make it available on the Internet to authorized parties through so called 'EPC Information Services' (EPCIS) (EPCglobal 2007). If an authorized player wanted to learn something about an object he or she would, therefore, not directly retrieve the information from a tag, but instead access available EPCIS online. The conglomerate of distributed EPCIS, their organisation and access management jointly form the "EPCglobal Network".

Because object information is accessed via a network, GS1's architectural vision for RFID has been characterized as 'data on network' (Diekmann, Melski et al. 2007). Of course, this architectural vision is in an early stage of development, and alternatives as well as complementary proposals exist. For example, some scholars propose that rather than storing relevant product information on the network it would be equally feasible to directly store it in the tag. In this way, data transmission cost and bottlenecks could be avoided ('data on tag' vision (Diekmann, Melski et al. 2007)). Equally, some industries have been deploying alternative RFID information services outside of GS1's EPCIS specification (for example, the company Afilias recently implemented RFID registry services for the aviation industry¹⁷). In order to provide this work with sufficient focus and reduce complexity the discussion, hereafter, will use GS1's 'data on network' architecture as the baseline of analysis and discussion.

3.1.3 Benefits and Critiques of RFID

Provided that RFID tags are embedded in everyday objects and accessible by a networked reader infrastructure, it will be possible to create myriad new information, tracking, and access services across industries. Today, RFID introduction is heavily promoted in the logistics environment. Here, it

read ranges by powering chips with higher Watt units than is legally permitted. UHF reader antenna design also dictates the tags read range. Conical antennas have a longer field than circular antenna attached to the same reader. Mirrors or other electronic field reflective material can be used to boost the read distance beyond the range of the antenna.

¹⁷ http://www.afilias.info/news/press_releases/pr_articles/2006-02-21-02

was shown that real-time assessment of product flows through RFID increases process efficiency, ameliorates supply chain control, reduces theft, shrink and out-of-shelf situations, and leads to less manual labour required. First experiences collected on the use of RFID in supply chains by the Metro Group showed labour cost reductions of around 11%, reductions of out-of-stock situations between 9% and 14%, and 11% to 18% less losses and shrinkages during transport and storage.¹⁸

Equally, RFID is increasingly used for seamless access controls: Ski-resorts use it as an entry to ski-lifts. Companies secure access to their buildings and corridors through RFID access cards. And public transport deploys the technology not only to manage the flow of people accessing and leaving the public infrastructure, but also as a means to facilitate the charging for transport services.¹⁹

In the mid-term, when the technology is ready to be deployed on the shopfloor, it can be used to improve marketing campaign management at the point of sale, boost the collection of useful marketing data available about people's activities while shopping, improve information services on the shop-floor, and facilitate dynamic pricing (e.g. charging less for products near the expiration date) (Jannasch and Spiekermann 2004). Also recycling of products and management of warranties and returns are simplified for retailers as well as customers. Many information and intelligent home services as those described in chapter 2 will reside on RFID technology's widespread deployment. And a recent study conducted in co-operation with the Metro Group revealed that even if consumers are informed about the potential privacy intrusiveness of RFID technology, they largely appreciate RFID based after-sales services. Figure 7 summarizes the findings of a series of two studies conducted by us which show that people judge RFID services as being beneficial to them and convenient.

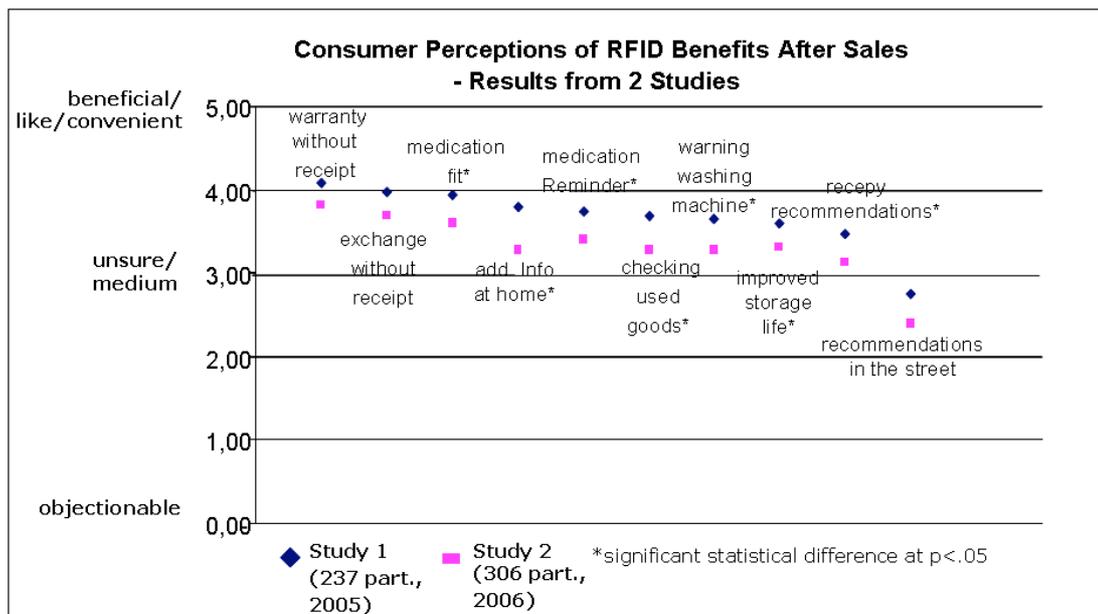


Figure 7: Consumer perceptions of after-sales benefits of RFID

However, even though RFID technology is such an enabler for many products and digital services, it also bears a number of social challenges. These include the impact of the technology on the job market once distribution centres and shops can replace warehousemen and cashiers with RFID readers

¹⁸ The Metro Group Future Store Initiative represented the first largescale rollout of RFID technology in a retail context in Europe. The findings were presented in „RFID Fahrplan der Metro Group“, Dr. Gerd Wolfram, RFID-Kongress für die Partner der METRO Group, Köln, May 14th 2004.

¹⁹ The London Underground can, for example, be used with the RFID based Oyster Card (see, for example, <http://www.idtechex.com/products/en/presentation.asp?presentationid=670>, last retrieved on August 28th, 2007)

(Federal Ministry of Economics and Technology 2007). Equally, the environmental impact of silicon vestiges in product waste is unclear (Koehler and Som 2005). Most prominently, RFID has been criticised by consumer rights organisations and the media for the potential privacy infringements it could cause (FoeBuD e.V. 2003; Center 2004). Some privacy advocates refer to RFID tags as “spy chips” (Albrecht 2006) and have rolled out public “STOP RFID” campaigns²⁰ against the technology’s introduction. In the US, a ‘Boycott Benetton’ campaign was launched upon the news that RFID chips would be embedded in the company’s clothes.²¹ Equally, the Metro Group decided to withdraw 10.000 customer loyalty cards upon the discovery of RFID chips in them by privacy rights organisations.²²

At the core of these critical voices are Class 1/Generation 2 RFID chips which imply that their information can be read out by anyone with a RFID reader in clear text in an uncontrolled manner and potentially unnoticed by an object owner. The German Association for Computer Science (GI) has therefore established a catalogue of provisions in order to minimize the potential dangers of transponders for citizens and society” (Pohl 2004). Equally, the OECD²³ and The United States of America Center for Democracy and Technology²⁴ have proposed guidelines for the application of RFID in areas where the technology interfaces with people.

Yet, at the same time, few insights exist on consumers’ real attitudes towards RFID and privacy issues surrounding the technology. Is privacy really such an issue to consumers in times where people start to get used to massive data collection in many other communication areas? Those investigating consumer privacy behavior in other electronic transaction environments find that privacy often seems to be less valued than privacy advocates proclaim. For the E-Commerce context, for example, (Spiekermann, Grossklags et al. 2001) found that even those people claiming to have the highest privacy concerns reveal the most intimate information about themselves and their preferences to online software agents. Continuously, surveys show that despite privacy being an issue for people, they rarely protect their personal data and electronic traces and also lack the knowledge and tools which could support them in doing so.²⁵

Against this background and experience in traditional electronic environments, the question arises whether consumers will really care about RFID undermining privacy and punish marketers who do not act according to privacy expectations. There is some temptation for retailers and consumer goods manufacturers to introduce RFID technology without any initial technical precautions and then observe how consumers react (Fusaro 2004). If RFID tags would neither be protected nor killed at store exits, but instead left unprotected, many after-sales service scenarios could be realized without consumers incurring any privacy transaction costs and without increasing the cost of RFID tags and infrastructure. Consequently, retailers are not sure of whether to leave RFID chips unprotected or demand the development and embedding of Privacy Enhancing Technologies (PETs) in the intelligent infrastructure created. Should they make use of the kill-function foreseen in the EPC Class 1/Generation 2 tag specification (EPCglobal 2005) and permanently deactivate tags’ functionality to transmit data when their customers 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 ‘locked’ in such a way that they are only accessible by

²⁰ <http://www.foebud.org/rfid>

²¹ <http://www.boycottbenetton.com/>

²² Computerwoche.de: „Metro entfernt RFID-Chips aus Kundenkarten“, 2.3.2004 (last retrieved on August 29th, 2007)

²³ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2006: http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1.00.html (last retrieved on July 20th, 2007)

²⁴ CDT Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology, 2006 (last retrieved on July 20th, 2007: <http://www.cdt.org/privacy/20060501rfid-best-practices.php>)

²⁵ Acquisti, A. and J. Grossklags (2005). "Privacy and Rationality in Individual Decision Making". IEEE Security & Privacy. 3(1): 26-33. found that around 70% of 116 US citizens interviewed know little or nothing about current privacy technologies. 67% never encrypted their mail and 83% never removed their phone numbers from do-not-call lists.

authorized entities thereafter? And if so, which PETs should retailers support? Should PET protection be applied by default or only upon customer demand? In order to answer these questions we have conducted a number of scientific investigations, both technical and sociological in nature. The following sections within this chapter will report on these investigations. They were carried out between 2004 and 2007 and centered around the following questions:

1. Which concrete concerns do consumers associate with RFID? (section 3.2)
2. Are these concerns technically and economically feasible and justified on the basis of current GS1 specifications? (section 3.3)
3. What technical options or PETs exist to provide consumers with control over RFID based information collection? (section 3.4)
4. How can the degree of ‘perceived’ control provided through such PETs be measured? (section 3.5)
5. Do consumers finally perceive control through the PETs proposed? (section 3.6)
6. Which PETs do consumers prefer and for what reasons? (section 3.6)
7. Is perceived control a major driver for PET preferences? (section 3.6)

3.2 Information Collection Concerns over RFID

Technical proposals to control the information flows created through RFID technology have been widely published in recent years. Chapter 3.4 below reports on over 177 scientific articles referenced alone on one single website dealing with privacy enhancing technologies for RFID.

However, no one seems to know exactly what concerns people. Do information collection concerns in the context of RFID relate to any read process occurring unnoticed and from a distance? Or do concerns about RFID relate only to readers collecting personally identifiable data? Potentially peoples’ concerns focus exclusively on highly personal objects the discovery of which could impact a person’s dignity (for example, underwear)? Or do people strive for a general “right to be let alone” from readers (Warren and Brandeis 1890)? (Solove 2006) points out that privacy concerns 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.

When conducting 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, we found that about 1/3 of print media messages and 40-50% of online media messages were related to consumer concerns and that this critical media reporting was on the rise in all media investigated (Falter, Günther et al. 2004). More precisely, 71% of consumer concerns 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, the themes raised are relatively unspecific to RFID technology. 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 concrete user concerns surrounding the introduction of RFID technology.

A first scientific study on RFID related consumer concerns was conducted by GS1's adjunct technical unit, the Auto-ID Labs (Duce 2003). 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, health, or privacy were brought up. The study concluded that privacy issues are indeed at the top of peoples' mind. More precisely, people rejected the idea of being tracked, of other people knowing what one buys and they believed that personal security could be at risk. A later study by consulting company Capgemini among over 2000 consumers in Europe and the US confirmed this result: In the EU as well as in the US, privacy related concerns dominate the list of consumer issues (Capgemini 2005). Interesting, in this study item-level RFID tagging is perceived by a majority of participants to have a greater impact on privacy than other technologies (including paradoxically even technical applications where RFID is used for access controls). Figure 8 summarizes these results.

Against the background of these general insights 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.

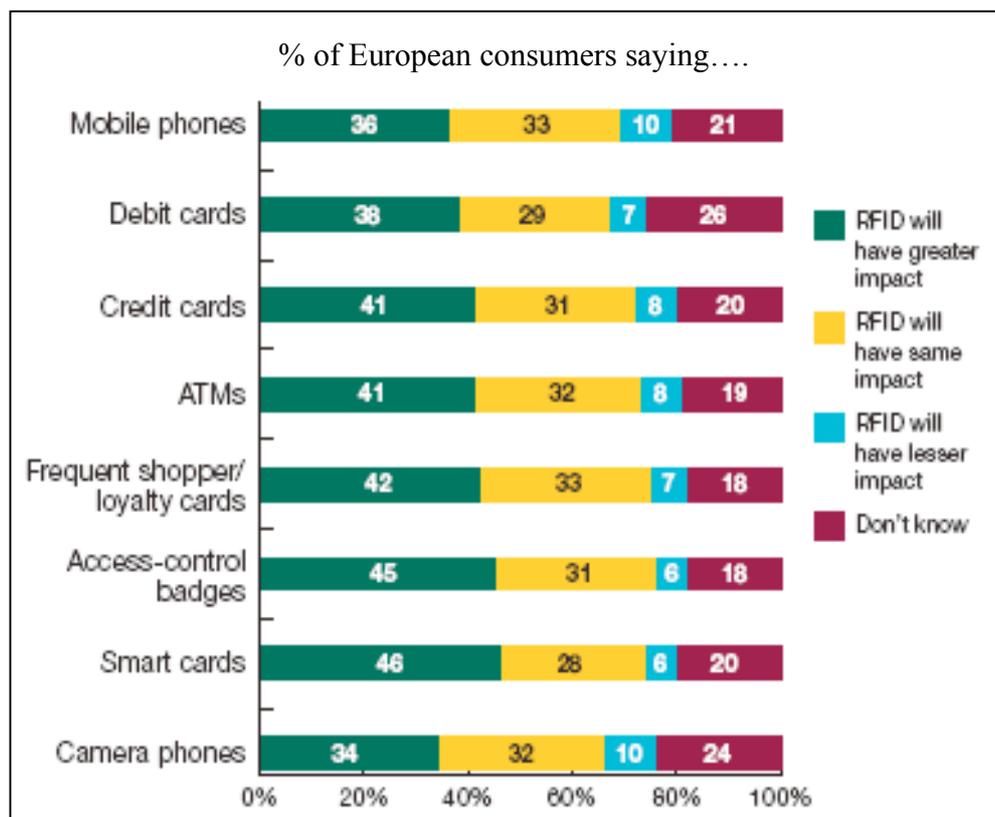


Figure 8: The Impact on privacy from RFID vs. other technologies (p.12, (Capgemini 2005))

3.2.1 Method: A Qualitative Approach to Elicit Consumer Concerns

Three focus groups were conducted in a Berlin test studio following the methodological outline proposed in (Krueger 1994). 8-9 Berlin citizens were recruited by a marketing agency for each session. 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. Loyalty cards were chosen as a starting subject because it relates both to shopping and data collection 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.²⁶ The moderator informed participants that many of the new services shown to them would be based on a technology called RFID. 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 (figure 9) and also the RFID deactivator machine (figure 10).



Figure 9: Automatic check-out of products tagged with RFID chips (Metro Group in 2004)



Figure 10: A Password based deactivator station for RFID tags

After this first film stimulus, participants discussed the benefits and drawbacks of the services they had seen and 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.

²⁶ The film material used has been produced by the Metro Future Store Initiative and can be viewed at: http://www.future-store.org/servlet/PB/menu/1007084_12/index.html (last retrieved on July 20th, 2007)

3.2.2 Results: RFID Related Consumer Concerns

The focus group set-up sought to understand user reactions to RFID upon full information about the technology's benefits and privacy 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 and concrete foci of potential concerns. The main issues which were echoed by the 26 participants in the 6 hours of discussion can be summarized as follows:

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

3.2.2.1 Concern of one's personal belongings to be assessed without one's knowledge and consent

The concern about unauthorized assessment of one's belongings reflects 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 assess 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?" and 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]..." This latter aspect has been confirmed by the Capgemini study as well: 52% of EU citizens and 42% of US citizens interviewed expressed the concern that tags could be read out from a distance (Capgemini 2005; van Lieshout, Grossi et al. 2007)

People seem to want to control the information that is being read out for distinct reasons: for instance, they fear 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 thief could, if you are not there, hold the reader to the window...and read and scan your apartment from a 10 metres distance.") or they plan how they could prevent the 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 (Pierce, Kostova et al. 2002). Psychology of ownership states that: "...control over physical environment stems from control of the object, control over the use of the object...social control stems from the ability to regulate others' access to or use of one's possessions." (p. 89 in (Pierce, Kostova et al. 2002). Not surprisingly 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."

3.2.2.2 Concern to become known to and classified by others

Participants echo another concern that the automated and large-volume collection of object data could be used to accumulate knowledge about individuals. Here, concerns relate to the awkward feeling of becoming 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”. Participants seemed to be afraid of a power-shift between them and those who own readers. They were concerned that, based on RFID data, they could be confronted with personalized advertisements. However, personalized advertisements were not criticized primarily due to the volume of messages (as suggested by the Capgemini study). Instead they felt uneasy with the possibility that 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’...”. In other studies, privacy scholars have found that people are indeed afraid of reduced judgements that others could make upon personal information (Smith, Milberg et al. 1996). RFID or UC environments generally seem to add the threat dimension of such judgments being publicly displayed.

3.2.2.3 Concern to be followed (tracked)

Being followed through the tracking of one’s objects refers to the possibility that object information is being read out and used to create movement profiles. Individuals’ whereabouts could be deduced 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.” The Capgemini survey confirmed that 55% of EU and 65% of US citizens would be afraid of tracking via tagged items (Capgemini 2005). Interesting enough, though, participants also seemed to distinguish different territories when they reflected on RFID tracking. In particular, they credited 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 use 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 which denies retailers the right to track individuals’ outside of their stores could be explained by humans’ innate territorial behavior which attributes limited individual rights to publicly shared space (Lyman and Scott 1967; Altman 1975).

3.2.2.4 Concern to be victimized

Against the background of these three concerns to be assessed, classified and followed, 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 their detriment 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.”

3.2.2.5 Concern to sign responsible for each object one owns

The concern to sign responsible for each object one owns was another concern raised by study participants. It is due to the potential 1:1 association of people to their objects through the serial number part of the EPC. People do not want to sign responsible for the misuse or fate of each object they own. For one thing, they fear the potential discovery of wrongdoings 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 creates 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.”

3.2.2.6 Concern about being restricted, educated or exposed through automatic object reactions

This concern relates to the possibility that RFID technology could be used to ‘paternalistically’ regulate peoples’ behavior by observing and correctively influencing their interactions with objects. RFID inherently bears the characteristic of object-object recognition. It can thus be used to 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’.” In another outlet we have reflected on this issue in more depth and under the term ‘technology paternalism’ (Spiekermann and Pallas 2005; Spiekermann and Pallas 2007).

3.2.3 Discussion: Requirements for RFID Information Flow Control

From a technical standpoint, all concerns raised by focus group participants could be interpreted as originating from a loss of control over three kinds of information flows: First, the information flow between individuals’ RFID tags and the reader infrastructure; second, the flow of information between objects, directly or via a network; and, third, the information flow happening at the backend of those entities collecting RFID data. Exercising control over these distinct areas of information flow seems out of reach for people. Some participants directly expressed their concern over the potential loss of control over their data: “...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?” And, indeed, this notion mirrors what Mark Weiser wrote early on when reflecting on the social consequences of Ubiquitous Computing: “The problem, while often couched in terms of privacy, is really one of control” (p. 694 in (Weiser, Gold et al. 1999))

To sum up, table 5 summarizes how the identified concerns can be related to the three distinct information flow areas and what kind of control requirements (both technical and organizational) are resulting against this background.

In line with (Averill 1973) (see section 2.3.2.1) we distinguish control requirements on three levels: First, cognitive control over RFID means that people need to be informed or aware of whether any of those activities they fear are really taking place. Cognitive control could be undermined if they did not know about the presence of RFID chips, be aware of distanced readers or not have any cues to see whether communication takes place. Beyond this loss of cognitive control, technological means would need to give people the possibility to exercise behavioural control over RFID and its information flows. This means that people would literally need to have an ‘off’-button which impedes any of the information flows from happening if desired. As will be discussed in section 3.4 below, some privacy

enhancing technologies which ‘jam’ or ‘block’ RFID reader-tag communication are going into this very direction. And finally, decisional control over RFID would mean that people have the right to opt out of information collection and processing activities. However, a perception of the effectiveness of such decisional control depends, of course, on consumers’ trust in retailers and all other parties involved in RFID data collection and sharing.

Table 5 gives a broad overview of how consumer concerns translate into control requirements. Here it becomes obvious that control over RFID related information flows is not only a matter of technological design, even though the next sections will exclusively focus on this area. The concrete reasons behind consumer concerns (such as psychology of ownership, territorial thinking, fear of negative classification and exposure) hint to some concrete steps retailers can take to avoid customer criticism. For example, retailers could demonstratively refrain from using readers in the semi-public spaces the control. More details on what retailers could do will be provided below.

Beyond such concrete steps, giving people the possibility to opt out of information processing at the backend and/or giving them access to the personal data held about them is an organizational and political decision marketers need to make (besides being a technical challenge for them with current IT infrastructures). If customers opted out of the processing of their data, marketers would have less knowledge about them, be less able to personalize offerings and risk to reduce the value of the intangible asset they hold through rich customer data. From a business perspective it therefore seems naïve to grant customers control over backend information flows beyond current legislation or restrain operations from processing customer data that could generate economic value. This economic rationale for using existing data as much as is economically and legally feasible is an argument for the importance of controlling information flows at those points where data is first created (Spiekermann and Cranor 2007). Thus controlling RFID tag-reader communication is key for those consumers who are sharing the concerns echoed above. Table 5 shows that control over RFID tag-reader communication is critical to address all consumer concerns except for object responsibility. For this reason, chapter 3.4 below will concentrate on privacy enhancing technologies which allow controlling this particular information flow within the RFID infrastructure. Before we analyse these concrete PETs for RFID, however, we first look into the technical details of RFID technology and investigate to what extent consumer concerns make sense and are justified against the background of current GS1 standards and visions.

Table 5: Consumer concerns, information flows and control requirements

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	<ul style="list-style-type: none"> • RFID tag – reader 	<ol style="list-style-type: none"> (1) Know about tag-reader communication (cog.) (2) Authorize tag-reader communication (dec.) (3) Impede tag-reader communication (behv.)
Concern to become known to and classified by others and be addressed respectively in public	<ul style="list-style-type: none"> • 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 	<ol style="list-style-type: none"> (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	<ul style="list-style-type: none"> • RFID tag – reader • RFID data flows at the backend: Combine RFID read points at the backend 	<ol style="list-style-type: none"> (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	<ul style="list-style-type: none"> • RFID data flows at the backend: Electronic identification data is combined with object data 	<ol style="list-style-type: none"> (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	<ul style="list-style-type: none"> • RFID data flows directly between objects (not possible with Class 1/Gen 2 tags) • RFID tag – reader 	<ol style="list-style-type: none"> (1) – (3)

3.3 Technical Feasibility of Consumer Concerns

Whether and how consumer concerns are technically feasible on the basis of current standards and economic rationale is a question we approached with the help of ‘attack-tree’ methodology based on (Schneier 1999). Attack-tree analysis can be used to systematically explore the technical feasibility of concrete consumer concerns. The distinct concerns described above are being set as potential ‘goals of attacks’ into the root of each attack-tree. Then these goals are hierarchically dissembled into sub-goals. Sub-goals need to be technically achievable in combination or alternatively. They are analyzed systematically to identify critical aspects of the technology. As described above, the analysis has been based on the assumption that GS1’s current standards and architectural network vision are embraced by the industry. A more in depth documentation of this analysis can also be found in (Spiekermann and Ziekow 2004; Spiekermann and Ziekow 2006).

3.3.1 Unauthorised Assessment of Belongings and Classification

We first identified the concern above regarding the unrecognized and unauthorised assessment of one’s belongings. For example, criminals could scan baggage at airports to identify valuable targets. Equally, merchants, in serving their economic interests, may electronically assess and better understand consumers in physical space in order to personalize offerings.

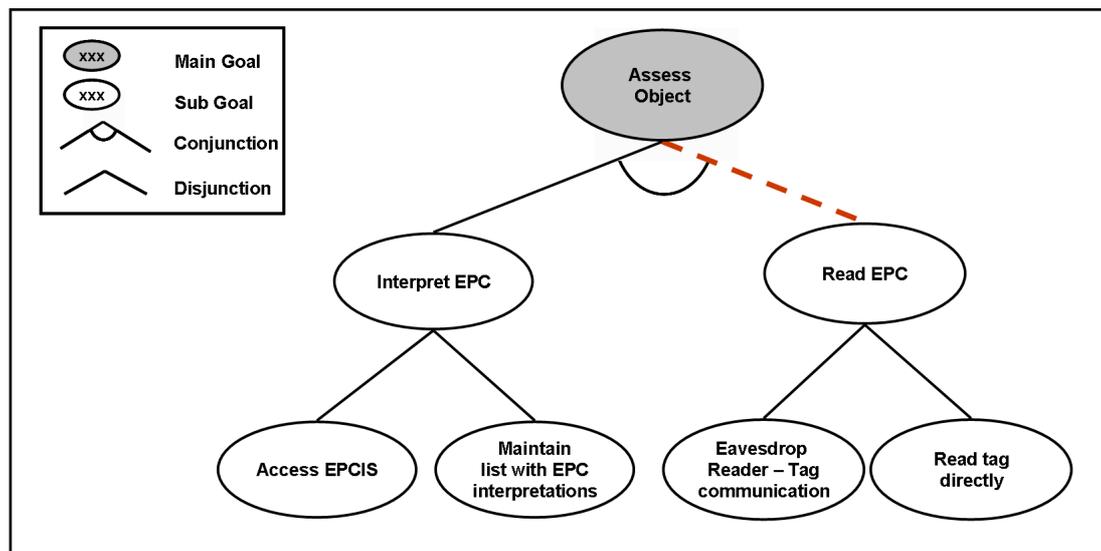


Figure 11: Attack-tree: Assessing objects tagged with an UHF RFID tag

We used the attack-tree above in figure 11 to show how the assessment of goods could be realized with the help of RFID. Two properties need to be fulfilled in order to seize objects unnoticed (and potentially unauthorized): (1.) The Electronic Product Code (EPC) which is stored on an RFID tag must be read out unnoticed, and, (2.) it needs to be interpreted. GS1 is propagating the use of passive EPC Class 1/Generation 2 tags operating in the ultrahigh frequency band between 860-960 MHz (EPCglobal 2005). These tags currently implement no protection against unauthorized access to the EPC. They transfer the EPC in clear text. Hence, the EPC can be read out directly by any RFID reader

from possibly a six to eight meters distance (dependent on the read equipment). This range is wide enough for attackers to scan objects unnoticed from a distance or track objects reliably at entry posts to public buildings and places.

Once the EPC is known it needs to be interpreted to determine what kind of object it labels. Figure 12 shows how the EPC is assembled (EPCglobal 2003). The part referred to as object class (item reference) is used for the numbering of a manufacturer's products. The attacker needs to know the link between these object class numbers and the types of products associated with them. Yet, this link is not a given. Manufacturers have their own company-internal numbering standards which they can continue using in the item reference part of the EPC. Consequently, the item reference number (and thus a large part of the EPC) is a 'non-speaking' number for those who are not acquainted with a company's internal numbering scheme.

Header	Filter Value	Partition	Company Prefix (EPC Manager)	Item Reference (Object Class)	Serial Number
8 Bits	3 Bits	3 Bits	20-40 Bits	4-24 Bits	38 Bits

Figure 12: The Structure of the Electronic Product Code (EPC)

However, as was outlined above, EPC Information Services (EPCIS) are envisioned to be created by every entity collecting data on a product (e.g. the manufacturer, but also logistics providers, distributors, etc.). This data can be put at the disposition of supply chain partners and other entities. Product manufacturers could build up EPCIS which contain extensive product information (e.g. product catalogue data) on a respective EPC and thus publicise the meaning of what is originally a non-speaking number. Assuming that product knowledge is accumulated in reference to EPCs along and (potentially even beyond) the supply chain, the use of EPCIS will, furthermore, provide extensive product lifecycle information (GCI 2003). In addition, languages are being developed to describe products and their attributes in a structured way. An example is the Physical Markup Language (PML) (Floerkemeier and Koh 2002; Floerkemeier, Anarkat et al. 2003). This language (once properly standardized) can be used to systematically describe the nature of a product. Finally, databases for looking up product information on the basis of EPCs may be established independently from the EPC Network and the retail industry. For instance, Greenpeace could maintain listings of gene-foods or rating agencies could publish the nature and quality of certain products based on the EPC.

The potentials to read out EPC information unnoticed and decoding its meaning shows that consumer concerns of having objects assessed unnoticed are realistic on the basis of current technical standards and proposals.

3.3.2 Tracking of Individuals via their Objects

RFID technology is believed to enhance logistics by enabling item-level tracking of objects (Bose and Pal 2005; Thiesse 2006). Once these objects are owned by individuals, though, the ability of tracking objects also becomes an ability to track their owners. Using RFID technology, retailers could track customers within their shops in order to create movement profiles which can be used to improve marketing strategies at the point of sale (Jannasch and Spiekermann 2004). In shopping malls several shops could combine tracks and analyse the popularity of different aisles. The state could have an

interest in the tracking of people in the context of criminal proceedings. Other purposes of tracking might be a company's interest in monitoring employees' whereabouts and working habits.

How tracking of persons can be done technically with the help of RFID, is displayed in figure 13.

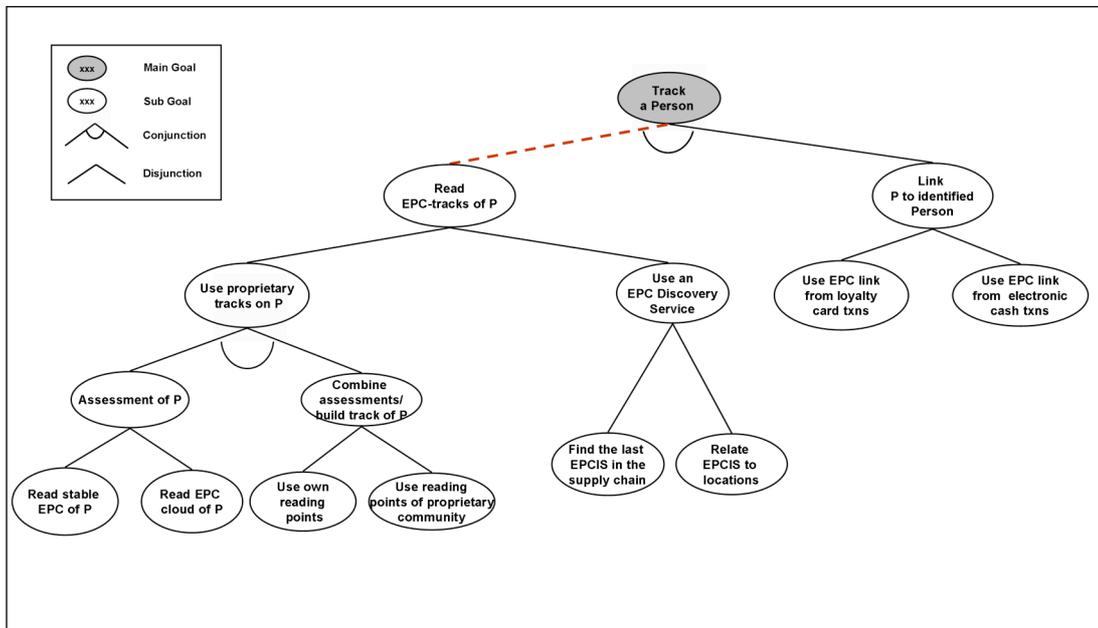


Figure 13: Attack-tree: Tracking persons

To track individually identified people, identification data has to be linked with individual tracks of movement. Identification data is collected when a person pays electronically or uses a loyalty cards. Secondly, individual tracks of movement need to be recorded and combined with their identity information. Product EPCs can be used – due to their unique serial number - as an identifier for the recorded tracks (denoted as ‘P’ in figure 13). They can be at the basis of proprietary tracks built through self-recorded read events of a collecting entity (i.e. a retailer). Or, they are used to retrieve tracks that spread across locations.

Assessment of EPCs (as described above) would be done for those objects which are regularly carried by a person over a longer period of time (for example, wristwatches or purses). This long-term EPC could serve as a kind of ‘cookie’. HTTP-cookies are strings of information used by web servers today to re-identify browser clients in the context of E-Commerce. In the RFID context, read events referring to EPCs in a similar way can be put in a sequence using reader timestamps and location data associated with its collection (Floerkemeier, Anarkat et al. 2003). As a result of this process, a track is established. If no long-lasting EPC is available, a ‘cloud’ of EPCs (EPC combination profile) could equally be used as a probabilistic identifier.

When tracking is desired beyond the premises of a collecting entity and is to be done on a regional or even global scale, the EPCglobal Network could possibly be used to gain access to geographically dispersed read event points. Dependent on the access rights of the data collector to the EPCglobal Network, read locations and times of an EPC could be retrieved from the EPCglobal Network querying for a product's last position. Verisign has announced an EPC Discovery Service which could be used for such purposes (VeriSign 2004).

All in all, the analysis shows that the current specification of the EPC (with a serial number part) and the EPCglobal Network technically allow for the creation of tracks if it is implemented in the way announced. However, establishing tracks across proprietary borders implies a need for access to the EPCglobal Network infrastructure. Within a legal framework this access right could be provided to GS1 member companies and governmental agencies. To what extent this will be the case, however,

and under what terms and conditions is a political and strategic uncertainty today. An abuse of the EPCglobal Network by some who unrightfully gain access to read events cannot be excluded technically if strong enough criminal forces are at work and succeed in hacking into individual EPCIS. However, if the EPCglobal Network keeps read-events distributed among its members it is questionable to what extent tracks can be established, because this would imply the necessity for an attacker to intrude myriad infrastructures; an effort which seems hardly justifiable for many attacks. Furthermore, much more efficient technologies are available to establish tracks of people, for example, mobile networks.

3.3.3 Making People Responsible for Objects

Public institutions could be interested in identifying owners of objects in the case of criminal investigations. Alternatively, if waste was found outside rubbish bins, those who pay for cleaning up might have an interest to fine the responsible person. The examples show that making people responsible for their objects bears some economic and social rationale. The attack-tree in figure 14 shows how a 'responsible' object owner could be identified with the help of RFID.

In order to hold people responsible for objects it is necessary to uniquely attribute an object to its owner or user. For this purpose, the EPC's unique serial number of an object would need to be read out and a link would need to be established with the one person who bought it. This link can only be established if that respective person paid for the object electronically and/or used a customer loyalty card in the context of purchase. Typically, an EPC would then be stored together with an object owner's name in some seller database and/or in the one of the loyalty card operator. An interested party (for example criminal investigators) could access the information set either directly from those parties where the object was sold or try to retrieve this information from the EPCglobal Network. For the latter to happen though, EPCIS would need to make the object-owner link accessible. Whether vendors are likely to do this on a regular basis is economically and legally questionable. For criminal investigations, however, the information may very well be made available.

A social and political challenge of this scenario is that the person identified as the object owner is always the last official object owner who has paid for an object. However, this person may not always be the holder sought after.

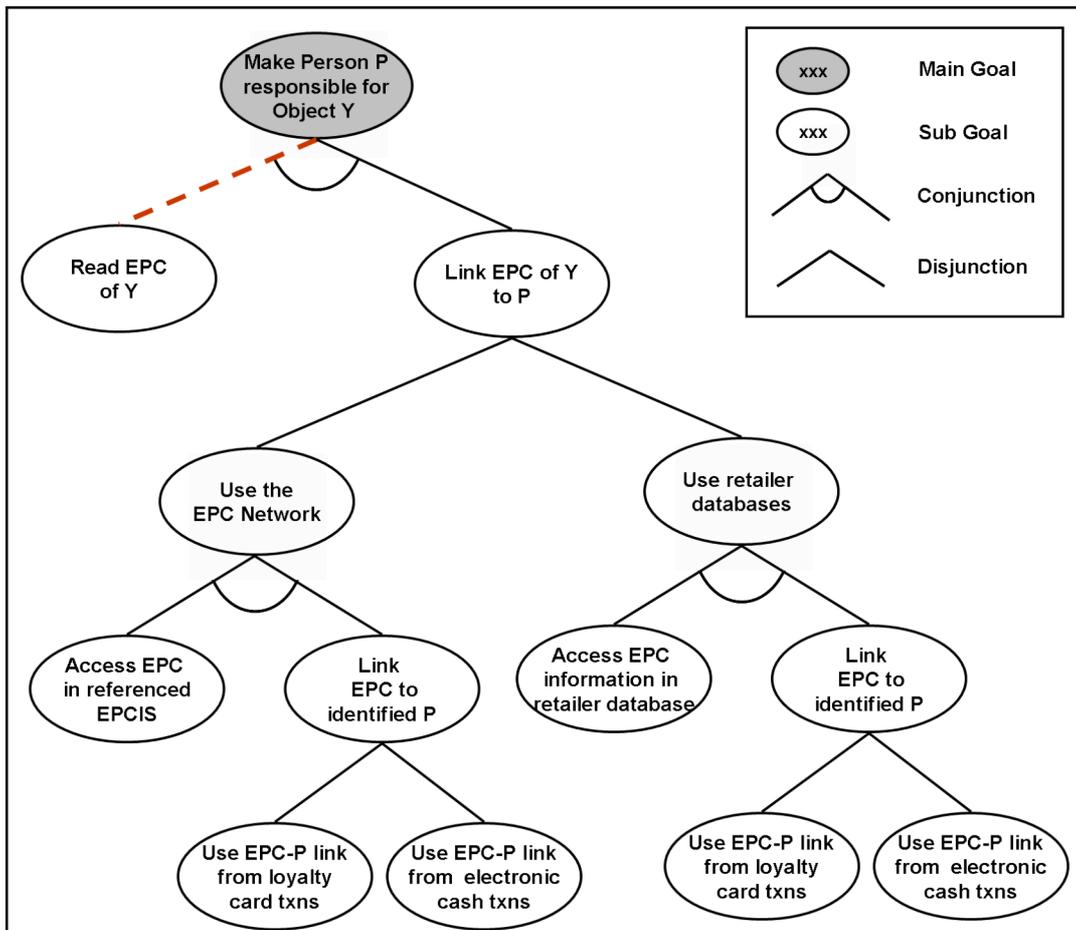


Figure 14: Attack- tree: Making people responsible for objects.

3.3.4 Being Restricted or Social Control through RFID

Social control refers to a fear expressed in the focus groups which was described as punishing or sanctioning actions of objects or systems as well as uncontrolled autonomous action of machines that cannot be overruled by object owners. A detailed reflection on this issue can be found in (Spiekermann and Pallas 2005; Spiekermann and Pallas 2007) and was provided also in chapter 2. Examples in the context of RFID include smart shelves in supermarkets which cause an alarm when a wrong product is placed in them, or cinema entries which automatically check visitors for drinks, snack foods or cameras brought with them, cars that force people to wear seatbelts by emitting noise, CD players that refuse to play records the copyright of which is unclear, or paper-garbage that starts to emit noise when a battery is by hazard put into it. How RFID technology can be used to implement this type of automated control is shown in figure 15.

RFID technology can recognize some forms of human misbehaviour by detecting the misplacement or the lack of objects. To do so, readers need to be installed at those locations where control is desired and be able to trigger some kind of signal in case misplaced objects are co-located.

A means to detect misplaced objects is to compare their EPCs with black-listed EPCs. Black-listed EPCs are those which should not to be placed at the location of read-out. Alternatively, a white-list could be used, containing EPCs explicitly allowed at the monitored location.

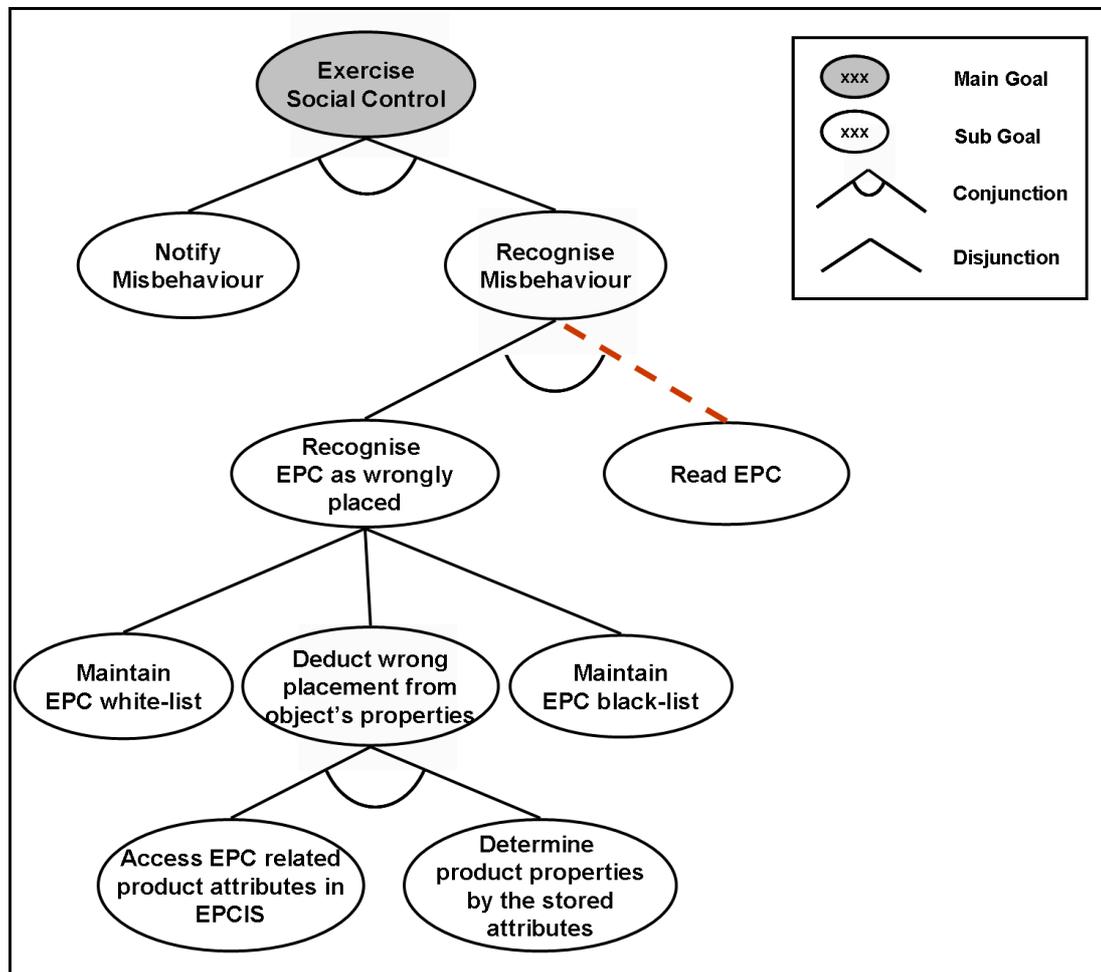


Figure 15: Attack-tree: Implementing social controls on the basis of RFID-labelled items

If such lists are not available, the EPC may be used to find out more about objects' attributes to determine whether or not they are allowable in a respective location. This description of objects' attributes might be accomplished in the long term through Physical Markup Language (PML). PML data about an object could potentially be provided by EPCIS and be accessible through the EPCglobal Network (Engels, Rivest et al. 2003). Checking for product characteristics online would, however, require a permanent connection to the Internet as well as access rights to the respective EPCIS. Whether such detailed product information services will be available in a standardized form, though, and at an affordable price is unclear as of today as is the economic feasibility of permanent availability of network connectivity.

Social control is thus technically feasible, but a realistic use of RFID for such purposes is probably limited to use cases where a manageable number of product combinations is involved and where the detection of false product combination or co-location is financially worthwhile.

3.4 Technical Options to Address Consumer Concerns

Attack-tree analysis shows that consumer protection is best served when EPC information is only read out in a controlled and authorized form after purchase. All consumer fears identified would become technically unjustified if access to unique EPCs was prohibited and/or under full user control. This logic is highlighted in section 3.3 through dotted hierarchical connection lines in attack tree figures. And also table 5 in section 3.2 has pointed to the strategic relevance of RFID tag – reader communication control if people want to maintain an upper hand over their data. For this reason, the current and subsequent chapters concentrate on technological alternatives proposed to avoid and/or control the information flow between RFID tags and readers.²⁷

The technical literature treating RFID security and privacy technologies has developed rapidly over past years. Table 6 gives a snapshot of 177 papers accumulated by one Internet site alone serving as a collection pool for scientific publications in this domain.²⁸ It contains literature from a wide collection of scientific conferences and journals with authors originating from all continents, and, for that reason, serves as a good source to gain a broad overview of the research conducted in this area and its emphasis of different subject domains. On the site, 123 out of the 177 publications listed (69%) investigate security and privacy mechanisms for RFID tag-reader communication. Of these, 71 (40% of the total) describe their main motivation as wanting to protect end-user privacy. In doing so, they are taking, however, different views and propose different ways in which user privacy could be managed. Referring mainly to this literature pool, as well as a few other sources²⁹, four major technological proposals can be discerned from a bird's view for the control of RFID tag-reader communication:

1. RFID tags are deactivated (software initiated tag ‘killing’) (EPCglobal 2005)
2. Readers communicate directly with tags which self-control access. We call these proposals ‘**On-tag Schemes**’, because they do not only require considerable on-tag security functionality, but also propose that tags decide about the release of data without user or agent intermediation.

²⁷ Analyzing individual attack-tree ‘leaves’ a number of other steps can equally be taken to technically address user concerns. These build on rigorous governance of the EPCglobal Network and a commitment (potentially embedded in codes of conduct) to technically enforced data scarcity. In particular, the storage of the EPC with its full serial number part seems to be a ‘key’ to abuse scenarios. Furthermore, reader data could be collected and stored at a level of granularity large enough to avoid reliable EPC based tracks and activity data relating to individual EPCs could be stored for a limited time frame. All these measures could be taken to thwart some of the potential privacy threats [Spiekermann, S. and H. Ziekow (2004). "Technische Analyse RFID-bezogener Angstszzenarien". Berlin, Germany, Institut für Wirtschaftsinformatik - Humboldt Universität zu Berlin: Spiekermann, S. and H. Ziekow (2006). "RFID: A Systematic Analysis of Privacy Threats and a 7-Point Plan to Adress Them." Journal of Information System Security 1(3): 2-17.]. The question is, of course, to what extent such measures are realistic in the light of economic interests and a vision of an Internet of Things which build on physical objects having digital representations.

²⁸ Website: ‘Security and Privacy in RFID Systems’ by Gildas Avoine. The website says to exclusively reference work “*which has been published in journals and conference proceedings, as well as technical reports, thesis, and eprints*” (p.1 in Avoine, G. (2007). "Security and Privacy in RFID Systems." Electronic Source. Retrieved June 6th, 2007, from <http://lasecwww.epfl.ch/~gavoine/rfid/>); <http://lasecwww.epfl.ch/~gavoine/rfid/#papers>

²⁹ Other sources include for example the publications of the AutoID Centre: <http://www.autoidlabs.org/> (last retrieved on August 24th 2007).

3. Users delegate privacy management to a privacy agent which mediates tag-reader communication based on general privacy preferences. We call such an approach '**Agent Scheme**' even though other scholars also use the terminology 'off tag' (Rieback, Crispo et al. 2005).
4. Users authorize each individual read-out process themselves (hereafter called '**User Scheme**').

Table 6: A snapshot of the scientific literature on RFID privacy and security

	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 <i>end-user</i> 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

In the following sections these four kinds of privacy enhancing mechanisms will be reviewed and we will discuss the extent to which they are challenged by technical, financial and user requirements; in particular, to what extent they are able to provide users with control over tag-reader information flows.

3.4.1.1 Killing RFID tags at store exits

The most straightforward approach to give people control over information flows between RFID tags and readers is to completely prohibit them. This can be achieved by simply killing RFID tags' ability to transmit information after the point of sale. Exercising the kill function could be done automatically (by default) as a step embedded in cashier systems. Alternatively, it could be offered to customers as a separate option apart from the main payment process.

From a technical perspective, the kill-function presents the most advanced privacy solution existing today since its properties have been integrated in the communication protocols for EPC Class1/Generation 2 UHF tags (EPCglobal 2005). It is the main privacy proposal made by GSI's adjunct technical laboratory, the AutoID Centre. Low cost tags are already available with the kill functionality. The main technical challenge associated with kill-commands is that they imply vulnerability for supply-chain transactions and point of sale operations if kill-passwords are not properly secured. If an attacker disposed of kill-passwords, he could deactivate RFID tag functionality and thwart all subsequent supply chain transactions.

Assuming that password distribution can be effectively organized and secured, the crucial drawback of the kill function is that it disallows any RFID based transactions beyond the point of sale.

Therefore, we do not believe that despite its technical advancement the kill-function can be the privacy measure of choice for industry. Many use cases are propagated by retailers today for after-sales RFID services.³⁰ These include long-term visions for smart home services, but also immediate benefits such as warranty and return management without receipts. All of these services – most of which are appreciated by customers (see figure 7 above) - would be impeded by the killing of RFID chips' functionality. Consequently, some scholars have argued “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)).

3.4.1.2 On-tag Scheme

Having seen the economic limitations of the kill approach, scholars have concentrated on the development of more sophisticated privacy solutions. 82% of the privacy enhancing solutions proposed could be characterized as an ‘On-tag’ Scheme. The On-tag Scheme foresees that only those RFID readers can access a tag which can authorize themselves vis-à-vis a tag (Feldhofer, Dominikus et al. 2004; Molnar and Wagner 2004; Ohkubo 2004; Batina, Guajardo et al. 2006). As a result, sufficient processing power and logic need to be implemented on the tag.

As the UML sequence diagram in figure 16 shows, such an authorization process would imply that a reader directly addresses an object's tag to ask for read permission and, if authorized, reads the tag's content. If the reader is operated by a 3rd party (for example, a mall or an airport), neither the object owner nor any mediating privacy device (see section 3.4.1.3) are involved in this process.

An early and relatively simple example for this kind of technology is the randomized hash-lock procedure proposed by (Engels, Rivest et al. 2003). It foresees that a tag implements a cryptographic hash function. When a product is sold, the tag's content is locked by storing on a tag a hashed randomly generated key k : $h = \text{Hash}(k)$. Both values h and k form a dataset (h,k) which needs to be known by any party wanting to unlock and access the tag in the future. When a reader attempts to access the tag, it sends a query and receives h as the tag's response. By looking up the corresponding k value in a back-end database, the reader sends k as an authentication response that is hashed by the tag; and, in case the resulting hash is equal to h , the tag releases its content.

The example shows that the functionality required to implement such a simple authentication protocol on the tag is quite complex: the tag would need to be able to compute a cryptographically strong hash function. Moreover, if the tracking of a tag via its h -value is to be avoided, then an even more sophisticated randomized hash-lock procedure would be needed requiring presence of a random number generator on the tag and imposing significant performance overhead on the back-end database (Engels, Rivest et al. 2003; Berthold, Guenther et al. 2005).

³⁰ A number of future home services have been demonstrated at CEBIT 2006 by the Metro Group: http://www.metrogroup.de/servlet/PB/menu/1044750_11/index.html (last retrieved on August 24th 2007)

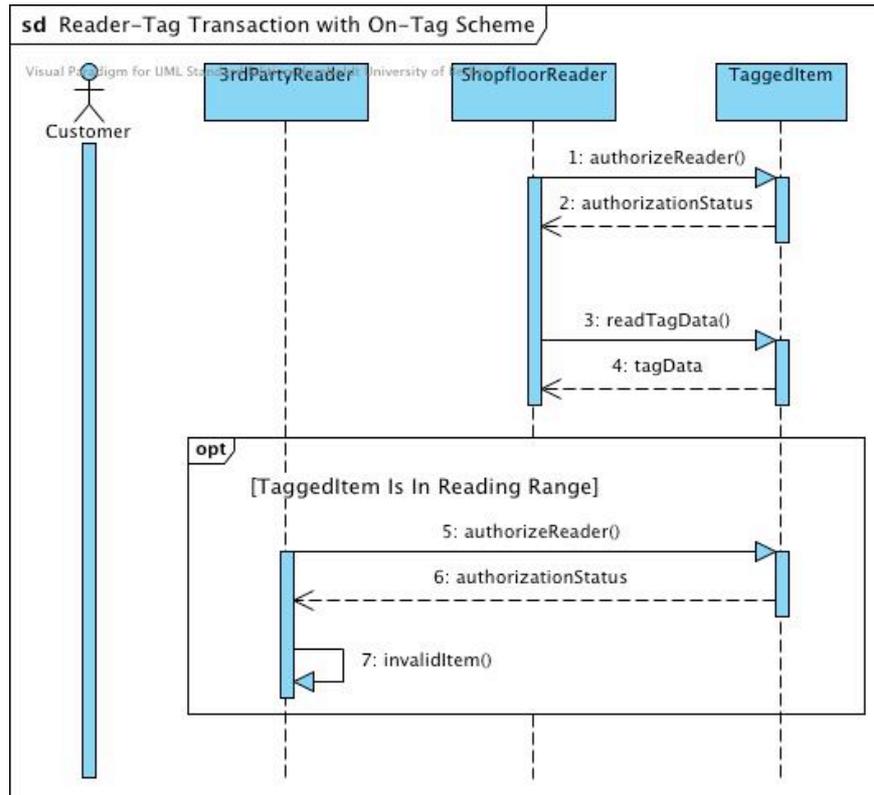


Figure 16: UML sequence diagram: RFID based communication in a mall, 'On-tag' Scheme

An alternative approach (usually used in such cases) which does not require any reader-backed communication is to rely on public key authentication algorithms. According to this approach the tag and the authorized reader store public and private keys correspondingly. In order to establish a communication session with a tag, the reader sends a notification and receives a random challenge generated by the tag. The reader uses its private key to encrypt the challenge and sends it back to the tag. By decrypting the received cipher text and comparing it against the original challenge, the tag verifies whether the reader possesses the required private key and establishes the communication session if the resulting plaintext is equal to the issued challenge (Figure 17).

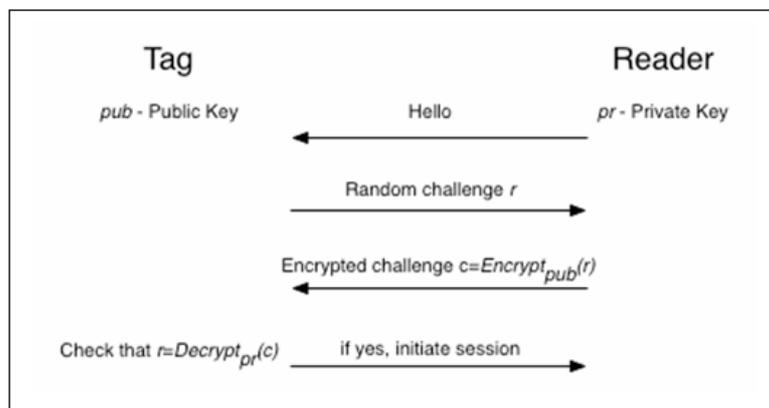


Figure 17: Challenge-response process for RFID tag-reader communication

Unfortunately public-key cryptography requires the tag to be able to perform complex mathematical computation. Considering extremely limited resources available in low-cost RFID tags, it may, therefore, be difficult to implement the public-key authentication on low cost tags. Table 7 shows the most compact implementations of basic cryptographic primitives currently known which could be suitable for passive RFID tags.

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)

The On-tag Scheme will require the tag to implement at least one of the listed primitives. This will inevitably increase the cost of the tag. (Lehtonen, Staake et al. 2006) argue that current RFID chips costing below \$ 0.50 dispose of 2.000 – 10.000 logical gates, only 200 – 2.000 of which are available for security needs. As can be seen from the numbers presented in table 7, this is not enough for being able to implement any of the mentioned authentication mechanisms. Assuming that Moore’s Law will hold also for RFID tags, the availability of low-cost tags capable of handling the listed algorithms may be a question of time. However, the cost vs. security dilemma should also not be underestimated (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).

Besides the fact that the On-tag Scheme assumes the availability of complex security functionality on tags, it also bears the challenge of key management. Assuming the availability of hash-based authentication mechanisms on low cost tags, parties wishing to access these tags are envisioned to maintain and constantly access private databases storing the (h,k) pairs (keys) or, generally, authentication rights. Furthermore, making stored data on the tag available to its current owners (e.g. buyers) would require the owner to have online access to the respective datasets. That leads to the question of how such key distribution and access can be managed in an efficient and trustworthy way. How can users ensure that keys maintained with retailers are not shared with 3rd parties or even the EPCglobal Network? No answer is yet being provided by RFID security researchers on this crucial question.

Another important drawback directly linked to the key management challenge is the sacrifice of any user control over tag-reader communications. According to the existing solutions for the On-tag Scheme, users are not notified of any read processes or read attempts taking place. If it is not the object owner himself who triggers the read process, but instead some other 3rd party reader, he or she would need to trust that only authorized readers actually access one’s tags. Therefore, once keys are accessible anywhere outside of the user’s sphere of influence, cognitive and behavioural control is sacrificed. Cognitive control is lost, because a user has no way to know when, where, and by whom he is read out. No device is foreseen to provide users with a-priori information about reading processes. And, even if the user knew, there would be no way in which he could stop the reading process from happening (exercising behavioural control). The UML sequence diagram depicted in figure 16 visualizes the On-tag Scheme. It shows how users are thus kept out of the loop of their tags’ activities.

3.4.1.3 Agent Scheme

Due to the drawbacks of the pure On-tag Scheme, such as high complexity, the necessity to use costly chips, little user control and the requirement of user-sided password (key) management, some scholars have started to suggest tag-reader mediation systems, potentially embedded in a PDA, which could assist users in their privacy management tasks. These solutions represent 11% of the publications reviewed. Early versions for such mediating systems have been suggested in the form of a “watchdog” device carried by users (Floerkemeier, Schneider et al. 2004). This device would inform users ex-post about reading processes that have taken place. Equally, scholars have suggested all RFID communication be blocked if a user desires so (Juels, Rivest et al. 2003).

Recently, scholars have started to go beyond an ex-post information (or notice) function as well as unspecific blocking of read processes and have instead suggested mediating privacy agents (Juels, Syverson et al. 2005; Rieback, Crispo et al. 2005; Rieback, Crispo et al. 2005). Mediation as it is outlined so far can either be realized by the mediating device serving as a proxy and emulating tag behavior (Juels, Syverson et al. 2005) or by selectively jamming reader-tag communication with the help of a ‘Privacy Guardian’ (Rieback, Crispo et al. 2005). For the former approach RFID tags, as a prerequisite, are cryptographically enabled and dispose of some centralized storage of RFID tag keys (as in the On-tag Scheme). In contrast, Privacy Guardian is a much simpler solution as far as tag complexity and key management is concerned (Rieback, Gaydadjiev et al. 2006). Privacy Guardian is envisioned to be embedded in a smart phone where it has enough power and processing resources to maintain a centralized security policy. This security policy dictates which RFID readers have access to which tags in which situations. It is implemented as an Access Control List (ACL) which manages RFID traffic based upon the querying reader (if it is known), the targeted tag(s), the attempted command and context data (i.e. location of the user). If a reader is not authorized to access a person’s tags, then RFID Jamming is used to block tags from answering reader requests. Selective RFID Jamming uses tag emulation to decode the incoming RFID reader query, determines if the query is permitted (according to the ACL), and then sends a short jamming signals which precisely blocks the timeslot in which the protected RFID tag would otherwise respond (p. 92 in (Rieback, Gaydadjiev et al. 2006)).

Three major challenges are inherent in the Privacy Guardian approach: First, Privacy Guardian’s jamming function only applies to deterministic tag-reader communication protocols which by now are not the standard any more for RFID Class1/Generation 2 tags. Second, users need to manually configure the ACL, specifying in advance their security policies (also called ‘privacy preferences’ by other scholars (Cranor, Dobbs et al. 2006)). This implies non negligible transaction costs for users as well as acquaintance with IT. The third challenge relates to context recognition. The Agent PET as described here needs to recognize when (time) and where (location) and under what circumstances (conditions, purposes) readers are allowed to access tags in order to apply a user’s security policies. However, how is the Agent PET supposed to understand and interpret context? Context sensitivity is a major and still unresolved research focus for Ubiquitous Computing scholars generally (Dey and Mankoff 2005).

In the concrete scenario of the Privacy Guardian it is foreseen that “context updates are provided either by users (via the user interface), or by authenticating “Guardian aware” RFID readers” (p. 98 in (Rieback, Gaydadjiev et al. 2006)). The latter implies that Guardian software would need to be a standard component of RFID readers, an assumption that is hard to be met by reality if Guardian software does not become a de-jure or de-facto standard. However, the approach makes plain that RFID standardization committees should generally consider to add space for authentication information to the RFID air interface. This would allow imbedding privacy enabling purpose information, such as fair information practices into the reader protocol (Floerkemeier, Schneider et al. 2004). As a result, Agent PETs such as the Privacy Guardian could become privacy context enabled.

Experience collected on E-Commerce Agent PETs which reside on similar preference specification procedures (such as the Platform for Privacy Preferences Project, P3P (Cranor, Dobbs et al. 2006)) has shown that generalized privacy rules are not always applicable to specific contexts (Spiekermann, Grossklags et al. 2001). Consequently, it may be that in some cases read-out processes occur or do not occur despite or against user permission. This possibility deprives users of full cognitive control or

knowledge about what is going on as well as behavioural control to intervene. This again can undermine trust in the protective abilities of the PET. As we will see in section 3.6.3 below anticipation of such system weaknesses can seriously impact the acceptance of RFID PETs. Only if protection mechanisms are enhanced over time and perform well upon user inspection, might users develop trust and believe they exercise behavioural control already by carrying the PET with them.

Figure 18 shows the sequence of transactions taking place between RFID readers, Agent PETs, tags, and users. It shows that in the long run users may be seriously relieved of transaction burdens beyond ACL configuration while still exercising technical control over their tags. If a lightweight approach can be found to precisely jam tag-reader communication for probabilistic protocols, it also circumvents the challenge of tag complexity and cost. Password or key management is simplified as the Agent PET automates it. All in all, the Agent Scheme can therefore be recognized as an important advance when compared to the On-tag Scheme. However, as the discussion has also shown, control perceptions of users over individual readout processes are still not optimal. Beyond the challenge of a trustworthy technical enforcement of privacy rules, tags are left unlocked by default. It is not the user who initiates a communication, but the network. As a result, the user is forced to trust PET performance to properly block undesired network requests. If the tag is locked by cryptographic means, then the Agent Scheme would be as expensive as the On-tag Scheme and sacrifice a lot of the charms of the lightweight jamming approach outlined above.

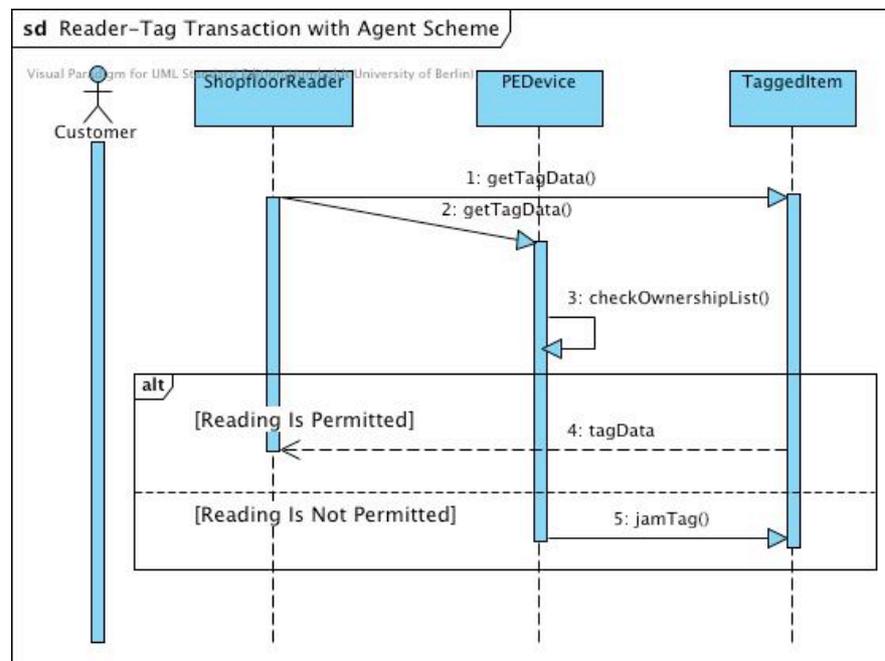


Figure 18: UML Sequence Diagram: RFID based communication in an intelligent mall, Agent Scheme

3.4.1.4 User Scheme

PETs for RFID may also be designed so that users exert immediate control over their RFID tags (Engels, Rivest et al. 2003; Engberg, Harning et al. 2004; Inoue and Yasuura 2004; Spiekermann and Berthold 2004; Berthold, Guenther et al. 2005). We have coined these solutions (which represents 7 % of the classified literature) 'User Scheme'. Solutions in this direction are proposing that tags are – similar to the On-tag Scheme - locked before people are leaving the stores with their tagged objects. Therefore, they do not a priori respond in any meaningful way to network requests. 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 give the tag explicit and situation specific permission to release its data to an interrogator (reader). The authentication process could be handled via a password scheme which we developed and extensively described in (Spiekermann and Berthold 2004; Berthold 2005; Berthold, Guenther et al. 2005; Berthold, Spiekermann et al. 2005).

In this scenario RFID tags are not killed, only deactivated at store exits, and the pre-configured kill-password coming with EPC Class1/Generation2 tags is being replaced at cash registrars with the personal password of an object owner. Object owners may in the simplest scenario possess only one password which allows them to manage their tags (analogue to other individual passwords they typically possess to access their e-mail, bank accounts or other sensitive electronic services). When an interrogating reader requests a tag's EPC, the tag sends a random challenge r to the reader. If the reader has access to the personal password p (e.g. because it is operated by the object owner himself), then it calculates a hash value $h = \text{Hash}(r, p)$ and sends h back to the tag. The tag performs the same operation and compares its internal h value with the one received from the reader. If the two values are equal, the tag releases its information. Figure 19 visualizes this process.

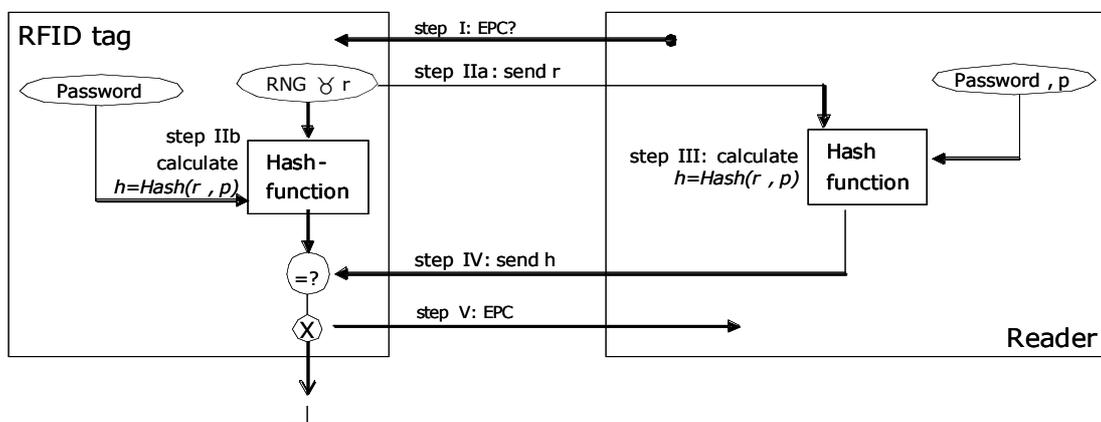


Figure 19: The Password Model (Berthold, Spiekermann et al. 2005)

The User Scheme puts the user in the role of the initiator of communication with the intelligent infrastructure.³¹ Before communication can take place, the user actively takes the context decision on whether he would like his object to release tag data or not. Theoretically, he thus has a high degree of control: cognitive control, because he is aware of the specific setting for which data exchange is about to take place and decisional control, because he can take the context dependent decision on whether he would like to open the reader-tag communication channel or not. Figure 20 visualizes the interface of the User Pet (on the left) as it has been captured in a film sequence on RFID PETs and opposes it with the Agent PET interface (on the right).

³¹ Initiation in this sense should not be confounded with the interrogator-talks-first (ITF) principle. Even if according to the EPCglobal standard readers always send out tag information requests first, the password model represents itself such to the user that he has to type in his password first before any data exchange can take place.



Figure 20: Visual Impression of User Scheme (left) and Agent Scheme (right)

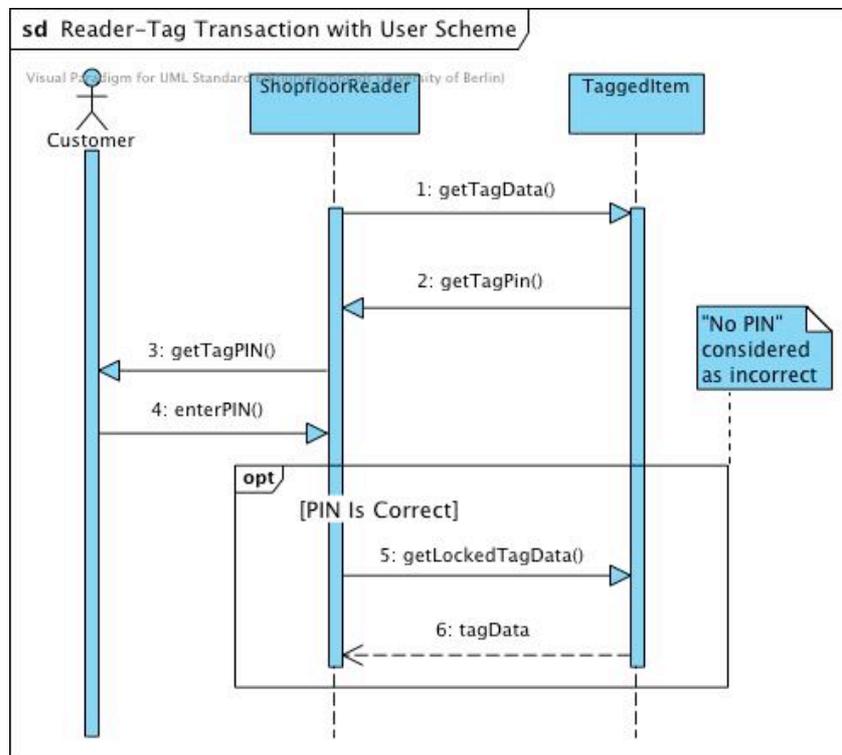


Figure 21: UML Sequence Diagram: RFID tag – reader communication in a mall, User Scheme

Two main challenges are associated with the User Scheme: One becomes apparent when studying the UML sequence diagram of the User Scheme depicted in figure 21: Pinning in passwords will leave users with considerable transaction cost each time they want to initiate a reading process (see number of inbound line for the user). This may be aggravated by users needing to memorize passwords. As far as password management is concerned, the existence of some user controlled password database may therefore be required if more security is desired (similar to the On-tag Scheme). In this case, the same key management problem outlined above for the On-tag Scheme would apply though. We, therefore, suggest sticking with a ‘good enough’ security approach in which people have only one privacy

password to all their devices. This password could be stored on a privacy card and could be amended by an extra four digits memorized by the user (Berthold, Guenther et al. 2005).

The second disadvantage of the User Scheme is that in order to offer high levels of security (and prohibit password eaves-dropping) it needs to embed the cryptographic primitives described above for the On-tag Scheme (a hash function and a random number generator). This drives tag cost. A simpler version of the User Model described by us would therefore not encrypt the password provisioning process. Instead, an authorized reader would directly send the password to the tag when requesting its EPC (Spiekermann and Berthold 2004). This solution would leave the user in control and be cost effective. Password sniffing by attackers – even though highly unlikely - could then, of course, not be prohibited.

Finally, it could be argued that the line between the User Scheme and the Agent Scheme may blur at some point when users generally possess reader devices. These reader device (similar to the Agent PDA) could contain algorithms which learn their owners' privacy preferences and subsequently automate individual password provisioning (ideally the way agents would operate). Indeed, this potential long-term merging of the two approaches is a viable scenario. However, the two schemes differ in that an intelligent RFID infrastructure evolving around a User Scheme may have different characteristics in the long term than an infrastructure evolving alongside an Agent Scheme. The User Scheme resides on the premise that people self-initiate each situation in which they feel that reviving a tag gives them immediate benefits. Consequently, read-out point would probably be limited to a few places where they provide benefits to people. In addition, a smart device used for accessing tags in limited circumstances would learn a user's privacy preferences on the basis of a series of 1:1 exposure decisions and people could be slowly led to delegate individual repetitive read processes to their read devices. In contrast, an intelligent infrastructure evolving around an Agent Scheme would most likely evolve in a similar way as today's E-Commerce infrastructures. People may be unwilling to specify and manage complex privacy preferences which they have to anticipate *ex ante*. This leads to an *a-priori* openness *vis-à-vis* collecting entities. This again could be an incentive for infrastructure investors to increase the number of read-points in order to collect more data.

3.4.1.5 Conclusion on current PET schemes

The analysis of the four privacy management models currently proposed for RFID shows that none of them is truly optimal. Trade-offs are inherent in each proposal in favour or against the level of security, the tag cost, key management complexity and user transaction cost. Furthermore, the level of user control achieved is very different from one solution to the other.

The On-tag Scheme is costly and complex in terms of key management, but it may be highly secure at some point. Most of the research efforts currently focus on this scheme, which may be justified on the background that the embedding of security mechanisms into low-resource RFID tags is an interesting engineering challenge, as such, and more knowledge in this domain may be a pre-requisite for other solutions (e.g. the Agent or User PET at some point to come). However, as was shown above, it isn't sensible from an economic and user perspective to concentrate on a pure On-tag Scheme to manage user privacy. Users are left in the On-tag Scheme with only one choice, that is, either to allow all parties having key access to read tag information or disable the tag. If the tag is disabled, they deprive themselves of after-sales services and neither they nor industry has any benefit from the sophisticated privacy solution on the tag. If they leave the tag enabled, they either deprive themselves of any further control over read-out processes (and privacy is effectively lost) or they require a key management PET that registers key sharing for all transactions. Once users need such a PET, though, the question arises why a more sophisticated Agent Scheme should not be embraced in the first place.

An Agent PET includes key management, but also aims to relieve users of the transaction costs implied in the privacy monitoring of individual transactions. It takes privacy decisions for users and, depending on its implementation, it can even be considerably less expensive, as far as tag cost is concerned. However, even though Agent PETs promise to relieve users from individual transaction monitoring, they also imply one major fallacy: They need to be able to make sound context decisions. Context decisions regard when and for what purpose RFID tag data should be revealed to whom. And,

furthermore, people need to trust that these context decisions are well done and in their best interest. If research in context sensitivity advances and if RFID standardization committees agree on embedding privacy related context data into readers, then smart RFID Privacy Agents could become an interesting technological option for users to gain control over RFID data exchange. However, current research in context modelling shows that people often need to serve as ‘mediators’ to enable proper context modelling (Dey and Mankoff 2005).

Therefore, the question arises why not to opt for a much simpler User Scheme from the beginning. Here, no a priori RFID tag-reader data exchange takes place. Only if users feel that they want to use a certain service they type in a password. A prime difference between this user driven solution and the Agent Scheme is that the user initiates the data exchange selectively and upon taking the context decision to interact with an intelligent environment. This kind of interaction design which puts the user literally ‘into the driver’s seat’ is conceptually close to the interaction paradigm of Near Field Communication (NFC). Here, users can only communicate with the intelligent infrastructure if they hold their small read-range tags or devices close to the service providing entity (Haselsteiner and Breitfuß 2006). The physical approach triggers the data exchange. In UHF-band long range RFID scenarios as we are discussing them here, this user initiated interaction paradigm is not a given. The interrogator-talks-first (ITF) principle embedded in the EPCglobal communication standard for Class1/Generation 2 tags (EPCglobal 2005) naturally foresees the intelligent reader infrastructure in a pro-active role vis-à-vis objects’ tags.

Assuming that privacy solutions will merge towards either an Agent Scheme or a User Scheme in some form, the question is: How much control do users want to exercise? Do they have a natural preference for the User Scheme since this solution gives them maximum control of RFID tags’ communication behavior? Or, do they wish to delegate such control functions to some mediating agents? Software agent literature generally suggests that users find it difficult to give up control and delegate sensitive decisions to agents even at the price of suboptimal decision making (Jameson and Schwarzkopf 2002; Diehl 2005). In the light of this question the next two chapters will investigate whether a User Scheme with a person actively and physically controlling tags in specific adequate situations will be more accepted and appreciated by users than the Agent Scheme. Does the User Scheme induce a stronger feeling of ‘perceived control’ in users than the Agent Scheme? And, how do these two privacy enhancing solutions compare with the simple, but presumably ‘written off’, kill function?

3.5 Measuring Perceived Control over RFID tag-reader communication

Chapter 3.3 showed that reading out RFID tag information, and in particular the unique EPC, is a core technical enabler for consumer concerns. Chapter 3.4 then described the technical alternatives developed today to manage the information flow between RFID readers and tags. In this and the next chapter we ask the question: Which one of these alternatives makes most sense from a user perspective, most sense, in particular, with a view to the end-goal of the consumer PETs, which is to give people not only ‘objective’ (technically proven) control over information flows, but also a perception of control over the information flow? PETs, if they are to protect individual people, should be considered consumer products. As such, they have to meet consumer expectations. In the case of RFID PETs, this means that they have to allow users to effectively manage their privacy through them. If people do not perceive that they are controlling their objects’ outgoing information flows by using any of the solutions above, there is not reason to use them and development efforts are in vain.

Yet, no research exists to our knowledge on how to measure the level of perceived control induced by the use of PETs, and in particular PETs for RFID. When engineers are designing tools to provide for ‘objective control’ over information flows, they therefore have no means to measure and test whether these actually meet the ‘subjective’ control desires of their customers (and thus market expectations). Also industry does not have any means to understand which technological option to support in order to maximise customers’ satisfaction.

Having seen the importance of control perceptions, the current chapter, therefore, reports on the development of scales which measure the level of perceived control induced by the use of RFID PETs. The type of control referred to here is the level of perceived control over the information collection process triggered by RFID environments. The chapter starts out in the next section with an overview of the control literature identifying those key diverse aspects of control which need to be respected in a measure to ensure its content validity. The chapter then reports on the development and testing of scales developed in line with these dimensions.

3.5.1 Dimensions of Perceived Control

As was outlined in chapter 2, sociology and psychology have identified control to be an important predictor for physical and mental well-being as well as for behavior. The construct has therefore been investigated by myriad scholars defining it from different angles and on different levels to the degree that (Skinner 1996) identified 111 different definitions for it. For scale development a reduction of this heterogeneous list of definitions is required. For this purpose two frameworks were chosen to concentrate on aggregated control dimensions for scale development. The first framework used to distinguish different aspects of perceived control is the one introduced already above and developed by (Averill 1973). Averill distinguishes between cognitive, decisional, and behavioural control. The second framework used here to discern different aspects of perceived control is the one introduced by (Skinner 1996). She thinks of control in terms of 'means-end' relationships. Therefore, she makes a distinction between the control one perceives due to the 'means' that one has at one's disposition to achieve some desired outcome. Furthermore, she recognizes the belief one has in one's own (or others') capability to effectively use these means (Skinner 1996). The latter construct is the belief in one's capabilities or self-efficacy (Bandura 1977). Skinner has termed this part of control perceptions as the belief in "agent-means" connections ((Skinner 1996), page 553).

The belief in means-end relationships has been substantiated by scholars viewing perceived control as contingency judgements. (Weisz and Stipek 1982) define perceived control in this sense as: "the degree to which the outcome in question is contingent upon variations in the behavior of persons like oneself" (p.241). If a PET is perceived as enabling such variations, for example by authorizing or impeding read processes, it may add to the notion of control in terms of contingency.

Another dimension of such means-end beliefs (or disbeliefs) is Seligman's construct of 'learned helplessness'. Learned helplessness is one of the first works on control (Seligman 1975). Together with Abramson et al. (Abramson, Seligman et al. 1978) he defined helplessness as "cases in which the individual ... does not possess controlling responses" (p.51) or does not believe any more in his or her ability to change things. Often due to negative experiences, humans enter into a stage of numbness where they feel that their activity does not impact the course of activities around them. In the context of RFID (or other UC environments) this would imply that people have given up trying to control information flows. With a view to PETs they may feel that their protection efforts are in vain despite the protection solution. In fact, the focus groups reported on above revealed some general helplessness thinking vis-à-vis the RFID infrastructure. It was reflected in statements such as: "I think that we cannot stop these processes. I am very pessimistic" or "...I think that we cannot avoid this. It will be introduced. Therefore, we can really only look into the question of how to think up a system with which we can eventually live."

Complementary to the belief or disbelief in the means of control is a person's trust in her own capabilities to use these means (agent-means beliefs). (Bandura 1989) called this aspect of control 'self-efficacy beliefs': "people's beliefs about their capabilities to exercise control over events that affect their lives" (p. 1175). Researchers in technology acceptance deducted the construct of 'ease-of-use' from this line of research (Davis 1989).

Finally, Skinner's framework identifies an 'agent-end' relation in the perceived control literature, a kind of direct belief in one's ability to control the environment regardless of any moderating means (Skinner 1996). This direct relationship is well reflected in feelings of power: "[Perceived control is]...the expectation of having the power to participate in making decisions in order to obtain desirable consequences and a sense of personal competence in a given situation" (Rodin 1990).

Feelings of contingency, helplessness, self-efficacy or power could all be classified as behavioural control (Averill 1973) because all of them can be considered as the belief of a person in the availability and mastering of a response to read-outs. However, as was shown above, (Averill 1973) distinguishes two further dimensions of control which are equally important to humans: cognitive and decisional control. In order to directly reflect these two dimensions in scale development, control definitions in terms of 'information' and 'choice' are additionally integrated into scale development. Langer propagates that people can only perceive control over situations if they are aware that they can influence these through their choices: "...control...is the active belief that one has a choice among responses that are differentially effective in achieving the desired outcome" (p. 20 in (Langer 1983)). In a UC environment this choice aspect would imply that people can opt out of being accessed by the intelligent infrastructure. In order to recognize choices, though, cognitive control is required. Fiske and Taylor (Fiske and Taylor 1991) argue: "...a sense of [cognitive] control ...is achieved when the self obtains or is provided with information about a ... event" (p.201). (Skinner 1996) refers to this type of control as 'information control'. In the RFID context information control would mean that people are made aware of being read out receiving some kind of notice or hint as to when and why readouts are taking place.

3.5.2 Scale Development and Item Testing

3.5.2.1 Control definition and initial item development

Based on the theoretical reflections above, scales have been developed to test peoples' perceived control over RFID reader-tag communication or, more generally, over being accessed by an intelligent infrastructure. The five dimensions of control, contingency, choice, power, information, and helplessness (the opposite of control) were taken as basic categories to formulate 14 questions capturing control perceptions (see table 8).

Following the guidelines of proper scale development (Churchill and Iacobucci 2001) a definition of the perceived control construct for the RFID/Ubiquitous Computing context was then formulated. This definition needed to capture the notion of control we desired to measure. Based upon a group discussion with four scientific experts, the following definition was conceived: "Perceived control [in a UC environment] is the belief of a person in the electronic environment acting only in such ways as explicitly allowed for by him or her."

We then took the 14 question items and assessed their relatedness with the control definition. For this purpose we conducted individual interviews with 25 participants (mostly students). Participants ranked the 14 questions in an order of decreasing relatedness to the control definition. Ten participants, furthermore, categorized the items into meaningful groups. Based on this ranking and classifying we were able to identify three questions being the least related to the control definition. We excluded these from further analysis. The resulting 11 questions promised a high degree of content validity and they also matched the control classification we had hoped to capture. Their importance ranking with regards to the control definition and their respective categories are presented in table 8, which, furthermore, includes four questions on self-efficacy or ease of use adopted from the Technology Acceptance Model (Davis 1989; Venkatesh 2000). The four items were added to the list of questions independently, because they have been extensively used in earlier studies and are proven to be good measures of self-efficacy beliefs in conjunction with IT use.

Summing up, six question categories with 15 items were assembled to measure perceived control. The next step was to investigate whether these categories would indeed show and be internally consistent when applied to a PET's use case.

3.5.2.2 Empirical item testing

129 subjects were invited by a market research agency to participate in a study on tomorrow's shopping environments. Sociodemographics of the participants was close to the German population.

47% were female and 53% male. 36% were below 30 years of age, 21% 30 to 39 and 43% 40 years or older. 40% had no A-levels and only 25% went to university. 81% had an income below € 30.000.

Table 8: Questions measuring perceived control over RFID tag-reader communication

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

The participants were split into two random groups. Group 1 contained 74 subjects. Group 2 had 54 participants. Both groups were presented with a film on future shopping environments in which RFID technology would be used (see annex 2). An effort was made to neutrally explain RFID technology. After-sales benefits of RFID were described on the basis of two services: an intelligent fridge and product return without need for a receipt. The film was identical for both groups except for the privacy enhancing technology (the PET) introduced as available to the consumer to control RFID tag's information flows after shopping. In group 1 the film briefing was such that RFID chips would all be switched off at the supermarket exit but could be turned on again with the help of a personal password if after-sales services (fridge, product exchange) would require. This film briefing is consistent with the User Scheme presented above. In group 2 the film briefing was such that chips would all be left on

at the supermarket exit but could only be accessed by readers for after-sales services if the reading purpose would match a person's privacy preference. This film briefing is reflecting the Agent Scheme as presented above in section 3.4.1.3. Before and after seeing a respective film, participants answered a battery of questions. The 15 control items were passed among other questions after the film. As depicted in table 8 they were answered on a 5-point scale pre-tested by (Rohrmann 1978) on their metric qualities. The film material, pictures and text, are included in appendix 2.

3.5.2.3 Internal consistency of control items

To understand whether the six control categories would really be reflected in the 15 control related questions, we first conducted a factor analysis. Assuming that there could be correlations between factors, we chose oblimin rotation. Prior to this procedure, missing items were replaced by mean values. Principal component analysis was employed. Factor analysis was first conducted for group 1 (User PET) and it was then analysed whether the results would replicate for group 2 (Agent PET). This first round of analysis showed that only 8 out of the 15 questions would consistently load for both treatments. Three factors with factor loadings above .6 could be identified. 2 items, one ease of use question and one question on contingency, saw very low loadings for both groups and, therefore, were eliminated from the item set. Five remaining questions, notably those on power and choice would not load consistently on the three separate factors or form their own proper and separate factors. In fact, for group 1 (User PET) power and choice related questions loaded together with information items. Group 2 (Agent PET) saw power and choice loading with helplessness. We therefore concluded that the items developed for power and choice would not be suited to reliably distinguish between factors and across different technologies and we therefore opted to equally eliminate them from the list of questions, well recognizing that content validity of the scale would suffer from this step. The remaining 8 questions were used again to first run factor analysis for group 1 and then (to confirm reliability) for group 2. In this step, three factors explaining the perceived control construct could clearly be identified for both PET samples. Tables 9 and 10 show the final factor loadings for the two PET treatments.

Factor 1 is clearly related to the category 'ease-of-use' of the PET (EOU1,2 & 3). Factor 3 is characterized by two highly loading items referring to 'helplessness' (HELP1, HELP2). Factor 2 is characterized by the items classified as 'information control' (INF1, INF2) as well as one question treating contingency (CON 1). Looking into the question text for the contingency item, we interpreted the loading as respondents' perception of their PET as an information source to determine further steps. Therefore, we regarded factor 2 as one dimension of control which measures the extent to which one perceives control as a consequence of being informed.

Tables 9 and 10 show that the cumulative variance explained through the three factors is above 78% for both PET conditions. Also, the three factors are almost not correlated which implies that they can be considered independent dimensions of perceived control. The final step was to investigate the internal consistency of the three factors. For this purpose we calculated each factor's Cronbach- α . The threshold of .8 was passed by the ease of use construct as well as the information control factor. The two items on helplessness, however, displayed a rather weak Cronbach α of around .6. This low level of internal consistency is potentially due to the fact that only two items were used to build the factor (typically at least three are recommended).

One noticeable difference between the Agent PET and the User PET is that information control items show positive loadings for the Agent PET and negative loadings for the User PET. We interpret this initial finding such that the User PET seems to have induced rather low feelings of information control in study participants. Indeed the film material shown (see appendix 2) did not contain an explicit reference to information being provided. Instead it was assumed that as users take context decisions themselves they are implicitly informed about the fact that a readout process will take place (because they trigger it). In contrast, the film showing the Agent PET explicitly showed a mobile phone informing the user about any readout event taking place.

Table 9: Reliability indicators of control scale (group 1: User Scheme)

Pattern Matrix - UserPET									
Factor Label	Item	Factors			Cron. - α	Culmulative Var. Expl. %	Corr.	Corr.	Corr.
		1	2	3					
Control through Ease of Use	EOU 2	0,954	0,048	0,021	.881	38,33%			.214
	EOU 1	0,881	0,065	0,094					
	EOU 3	0,854	-0,162	-0,088					
Information Control	INF 2	-0,114	-0,918	0,046	.837	64,30%	(-).243		
	INF 1	0,077	-0,855	-0,067					
	CON 1	0,068	-0,822	0,025					
Helplessness	HELP 2	-0,109	-0,014	0,905	.650	78,64%		.110	
	HELP 1	0,165	0,001	0,800					
Extraction Method: Principal Component Analysis. □ Rotation Method: Oblimin with Kaiser Normalization.									
Rotation converged in 5 iterations.									

Table 10: Reliability indicators of control scale (group 2: Agent Scheme)

Pattern Matrix - Agent PET									
Factor Label	Item	Factors			Cron. - α	Culmulative Var. Expl. %	Corr.	Corr.	Corr.
		1	2	3					
Control through Ease of Use	EOU 2	0,933	0,058	0,021	.915	35,44%			(-).063
	EOU 1	0,924	-0,044	0,041					
	EOU 3	0,912	0,025	-0,062					
Information Control	INF 2	-0,066	0,875	0,026	.836	61,44%	.119		
	INF 1	0,025	0,866	-0,007					
	CON 1	0,087	0,836	-0,024					
Helplessness	HELP 2	-0,070	0,167	0,867	.579	78,63%		(-).094	
	HELP 1	0,073	-0,185	0,809					
Extraction Method: Principal Component Analysis. □ Rotation Method: Oblimin with Kaiser Normalization.									
Rotation converged in 4 iterations.									

3.5.2.4 Conclusions on scale development

Scale development resulted in the identification of measures loading on three distinct factors to measure perceived control over the intelligent infrastructure through the use of a PET. The first dimension of control identified relates to control through self-efficacy. As people believe they find it easy to use a PET, they also feel more in control. The second dimension of control relates to information. Factor loadings show different signs for the two technologies indicating that information control may be perceived differently depending on the PET technology. However, high factor loadings and Cronbach- α values above .830 indicate that, regardless of the technology the three items identified form a representative scale to measure information control. Finally, the opposite of control, a feeling of helplessness turned out to be relevant to measure the potential failure of PETs.

3.6 RFID PET Acceptance and the Relative Importance of Perceived Control

The above sections have outlined consumers' concerns over RFID technology. These could cast a cloud over the benefits and services enabled through the technology and, as a result, should be addressed effectively. The question is, which one of the current PETs proposed makes most sense from a user perspective? Chapter 3.5 has expanded on the psychology of perceived control and has presented the development of a measure suited to investigate the degree of control users perceive over the intelligent infrastructure through PET use. Is the Agent Scheme or the User Scheme more preferred by future consumers? Or potentially none of them appreciated?

From a theoretical perspective the User Scheme as described in section 3.4.1.4 should induce a user of RFID technology with the highest levels of control. It should do this because the User Scheme envisions a passive RFID infrastructure in which RFID tags are deactivated by default and are only 'switched on' for specific purposes in which a consumer wants to take advantage of available services. The user is thus in the driver's seat. He does not have to delegate control to an agent which jams 'open' tags answering to a pro-active reader infrastructure. He also does not have to care about uncontrolled key-sharing practices as they may occur in the On-tag Scheme. Instead, consumers have full control over their tags' activities while still profiting from the advantages of after-sales RFID benefits. Yet, taking a step back, the question arises whether consumers want to engage into any such control activities (regardless of the Scheme). Perhaps they simply want to kill chips and forgo potential after-sales benefits?

Some scholars have noted that RFID technology may not bear enough benefits for consumers to justify any cost associated with RFID (Duce 2003). Agent and User Schemes imply some consumer investment in terms of transaction costs (to use them) and potentially also financial cost to buy and operate them (in the Agent Scheme). If this is true, it may indeed be that consumers will prefer a straight out killing of RFID tags at store exits. This solution can be implemented with reasonable effort based on current standards. Yet, as was shown above, economic rational would call it a dead-end as marketers want to offer after-sales services.

The current chapter therefore investigates how important RFID after-sales benefits are for consumers and whether such usefulness reflections will drive their acceptance of the PETs proposed. It seems rational to expect that consumers who appreciate after-sales RFID services would prefer to know they are in control while at the same time 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.

Given the theoretical superiority of the User Scheme, in terms of control, it furthermore seems sensible to expect that users will perceive more control over RFID tags' communication when being confronted with a User Scheme than when delegating control decisions to an agent. 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.

A major premise of H3 is, of course, that User PETs are indeed perceived as superior by their users. Do they really (in line with our expectations) induce a higher level of perceived control in users than Agent PETs? To answer this question we hypothesize:

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

Beyond a pure comparison of the protective options it is also of interest to understand the dynamics behind the use of complex PETs. We refer to 'complex' PETs here because Agent and User Schemes imply more transaction costs for users than the kill function does. As was outlined above, retailers have an interest in not killing RFID tags. As a result, the drivers of user acceptance of more complex PETs need to be understood. Which one of the three control dimensions identified in chapter 3.5 are most determinative for users' judgements of the respective PETs? 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.

In addition to this control perception of complex PETs, theory of reasoned action (Fishbein and Ajzen 1975) would suggest that other attitude elements and peer opinions (subjective norm) can play a role when humans determine to 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 (Ajzen 1985; Ajzen and Fishbein 2005). 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 complex 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 (Rogers 2003). If people have these characteristics, they 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 (Rogers 2003). 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.

3.6.1 Method Used to Investigate User Perceptions of RFID PETs

3.6.1.1 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 (study ②). Participants for this study were recruited according to the same demographic parameters but included urban citizens from four different German regions.

In both studies, participants were briefed to participate in a research 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.

The film material used in these two quantitative studies used a different material than the ready-made RFID documentations in earlier focus groups. It was exclusively produced to inform people in a neutral manner about RFID services as well as the different potential PET solutions envisioned by engineers. The different options at store exits (kill chips, 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 2 for the different briefings on the Agent and the User Scheme).

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 the complex PET shown to them 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 11 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 3 details the items used to measure these constructs.

Table 11: 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	

3.6.1.2 Film stimulus

The film stimulus began 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 simultaneous of use sly 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 (similar to the configuration required to set up the ACL list in the context of Privacy Guardian). The reader network would then exchange privacy preferences with the mobile phone agent. The phone serves as a Privacy Guardian in this scenario.

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 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).

3.6.1.3 Measurement constructs

The dependent variable used to test hypotheses 1 through 5 was measured by using one final question asked at the end of the second questionnaire which used an 11-point scale from 1 (totally destroy chips) to 11 (deploy chips with PET) and read as follows: “Former questions and the film showed that RFID technology can bring about both disadvantages and advantages for consumers. Of course it would be possible to totally destroy chips at store exits instead of using a <password protection scheme>/<mobile phone computer>. What would be your overall assessment in this regard? Please mark your tendency on the following scale.”

The independent variables influencing this assessment in study ① included the perceived usefulness of RFID after-sales services (USF) and the anticipated ease of use of RFID generally (EOU), peer opinion on RFID and perceived control through 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 (ATT), technical affinity (TA) and privacy attitudes (PRIV).

Usefulness of after-sales RFID services (USF) was measured with the help of a 9-item Likert scale summarized in table 12. For the two PET groups the usefulness of RFID services was measured after the film. For the group which learned about chips being killed, the usefulness of potential RFID based services was measured before the film was shown. Perceived ease of use of RFID (EOU) was measured with 3 items deducted from former technology acceptance studies (Venkatesh 2000). Technical affinity (TA) was measured by employing a 4 item scale taken from (Baier 2004).

In terms of privacy sensitivity, two distinct groups can be discerned which hold different attitudes towards the type of data distributed: those who are more concerned about revealing profile information (such as hobbies, preferences, etc.) and those who are more concerned about identification data (such as physical addresses, phone numbers, etc.) (Spiekermann, Grossklags et al. 2001; Berendt, Guenther et al. 2005). We expected profile concerned users to worry more about RFID as the technology allows more directly for the creation of profiles and less so for the collection of identification information.

Two items derived from the Theory of Reasoned Action were used to measure peer opinion: “People who influence my behaviour will think that I should use RFID” and “If my friends knew about RFID they would recommend me to shop in the supermarket of the future.”

Equally, a new 4-item scale was developed to measure the attitude towards new technologies in general. This scale asked participants whether they felt that new technologies would render every day life easier or more complicated, whether humans would be overrun by new technologies or whether they felt that new technologies mean positive progress for human kind.

Finally, perceived control through the PET was measured in study ① as described above by employing the three factor scales which distinguish control in terms of ease of use of the PET, feeling in control due to being informed through the PET and as an opposing factor, feeling out of control or helpless despite the PET. In study ② the same scales were extended and improved by adding a few additional items and fine-tuning the wording of items. These changes were driven by the poor Cronbach- α results for the helplessness construct in study ① (described above in section 3.5.2.2). By using four new items to this scale, internal consistency could be improved in study ② (see table 14). Also 2 items were added to the information control scale in study ② and replaced the one original item categorized as measuring contingency control. This change did not lead to an improved internal scale consistency in study ②. For future studies we would therefore recommend to stick with the ease of use and information scales presented in chapter 3.5 and complement these with the four new helplessness items used in study ②. The details of these amendments can be inspected in appendix 3.

3.6.2 Results: How do Users Respond to PETs for RFID?

3.6.2.1 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 12). 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 (User and Agent PET) were split into two groups depending on whether their usefulness ratings were above or below mean group average. We 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 valued the PET on average at 5,61. Those expecting less benefits from RFID valued 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 12: 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 we 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 statistically 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 the control perceptions raised through the two PETs. For the reasons outlined above we hypothesized that the User Scheme would lead to higher perceptions of control than the Agent Scheme (hypothesis 4). As table 13 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 rather easy to use (which was suggested by the two films). Furthermore, they perceive information control to be on a medium level. These findings have also been reported on in (Guenther and Spiekermann 2005).

Table 13: 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 perceived control, usefulness, ease of use of RFID and the role of personal variables for preferring one or the other PET scheme. For this purpose multiple regression analysis was conducted. Table 14 gives an overview of the results obtained.

All three regression models summarized in table 14 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 R2 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 seeing 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.

The regression models reveal 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 Agent PET if their peers are in favour of using RFID. In both groups, a perception of helplessness reigns and 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. This is surprising seeing that a major value proposition of the Agent Scheme is supposed to be the PET's ability to record and show RFID tag-reader communication processes. Yet, at the

same time, delegation of decisions and minimization of personal transaction cost could have led the study participants to not consider information as something outstandingly positive or negative about the Agent PET.

Also, and interestingly, peer opinion seems to be a driver for Agent PET acceptance. In contrast to the User Scheme where the user must trust in his own judgements, the Agent Scheme seems to be driven by the judgement that others play in one's protection device. This makes sense as the trust literature also provides some indication that trust can be 'inherited'. If one's peers appreciate RFID services and recommend their use while using Agent PETs, then one's likelihood to adopt an Agent PET increases as well. Unfortunately, a limiting restriction to this finding is the low internal factor consistency for this construct.

Finally, when personal variables were added to explain the preference for the kill function or the User PET in study ②, 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 and yielded no impact on the adoption of PETs.

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.

Table 14: Regression analyses: Divers for preferring the kill-function over a complex PET

PET scenario	Study ①								Study ②			
	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	<i>a</i>	<i>β</i>	Sig.	no of items	<i>a</i>	<i>β</i>	Sig.	no of items	<i>a</i>	<i>β</i>	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

3.6.3 A 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 study ②. We analyzed the reasoning for preferring a complex PET or rather killing tags with the help of a content analysis (Kassarjian 1977). 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 15.

Table 15: Main themes for participants when opting for a User PET instead of killing 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
<i>TRUST related reasons against User PET</i>	<i>76 (70%)</i>		
consequences for society	23	2	0
other	6	0	1
transaction cost of the password scheme	3	1	0
lost RFID benefit through kill	0	11	16
appreciation of the PET	0	1	8
transaction cost to kill	0	1	5
person is unconcerned	0	0	1
passive resignation	0	0	2

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 some remaining recognition or scanning. These findings clearly hint to the importance of trust building mechanisms such as 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 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 through the User PET. Some participants (18%) finally were stuck in the middle in seeing RFID benefits on one side, but equally mistrusting the PET solution.

3.6.4 Conclusions on the Acceptance of PET Solutions

The main finding from the comparative PET study is that complex PETs as they are envisioned today by many UC 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 privacy subject for the UC research community.

Content analysis suggests that users are looking for highly trustworthy and straight forward solutions to privacy. Solutions which 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 RFID privacy engineering.

The question is, of course, how precisely engineers can work towards signalling trust through the PETs they build. This work does not provide an answer to this question. However, some insights have been gained in recent years in the E-Commerce context on how trust can be enhanced through technical mechanisms (Chen and Dhillon 2003; Grabner-Kräuter and Kaluscha 2003). (Patrick, Briggs et al. 2005) accumulated 15 'Trust Design Guidelines' (table 16). The challenge is that these works are residing on the notion that people are using some display to access electronic services while Ubiquitous Computing is driven by the 'calmness vision'. However, both the Agent Scheme and the User Scheme imply the existence of a control device and/or a reader with a display that is operated by users. This device could record RFID tag-reader transactions and could potentially serve to embed some of the trust signals as they are summarized in table 16 for another context. The existence of such a device, however, also challenges the calmness vision of UC. If information collection about people cannot be fully automated because people want to control information flows, then the vision of calmness (inherent in such proposals as the On-tag Scheme) must be questioned. And, in contrast, it must even be asked whether the attention one would need to invest into any PET would really be worthwhile the benefits derived from RFID services.

Finally, another surprising 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 (even though the direction of influence is unclear from the results). This goes in line with our arguments for trust building communication and signals embedded in users' read devices. 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. In contrast, Agent PETs do not seem to underlie the same dynamics. If Agent PETs 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 placed in the Agent PET seems to increase. Rules 7 and 9 of the trust guidelines in table 16 also hint to the importance of peer evaluation. If an Agent PET carried a trust seal and if peer evaluations were available on Agent PETs' performance or Agents provided hints as to the trustworthiness of a respective RFID enabled environment or service rating, then people may be more apt to adopt it. Analogue to recommendation sites on the Internet which rate the quality of offerings, it may be realistic to anticipate mobile devices which give recommendations on and additional information concerning physical space. Consumers can thus detect 'augmented reality' services at their disposition. In the course of such service use, trust ratings could equally be given to users alongside service recommendations and reviews. A simple example from the E-Commerce context doing just this is the Privacy Bird application (Cranor 2003).

Table 16: Trust Design Guidelines for E-Commerce Sites

Guidelines
1. Ensure good ease of use
2. Use attractive design
3. Create a professional image – avoid spelling mistakes and other simple errors
4. Don't mix advertising and content
5. Convey a 'real-world' look and feel
6. Maximise the consistency, familiarity, or predictability of an interaction both in terms of process and visually
7. Include seals of approval
8. Provide explanations, justifying the advice or information given
9. Include independent peer evaluation such as reference from past and current users and independent message boards
10. Provide clearly stated security and privacy statements, and also rights to compensation and returns
11. Include alternative views, including good links to independent sites within the same business area.
12. Include background information such as indicators of expertise and patterns of past performance
13. clearly assign responsibilities (to the vendor and the customer.
14. Ensure communication remains open and responsive, and offer order tracking or an alternative means of getting in touch.
15. Offer a personalized service that takes account of client's needs and preferences and reflects social identity.

The present research is limited in 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 (Adams and Sasse 1999). Different results may have been obtained if the User Scheme film had shown, for example, biometrics as the authentication mechanism. Equally, the agent scenario could have shown an agent embedding more trust mechanism in its design (Maes and Wexelblat 1997). 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 or delegated communications in general. More research is needed to 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 would 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 (Sheeran 2002; Ajzen and Fishbein 2005; Berendt, Guenther et al. 2005) (mean correlations are around .53 according to (Trafimow, Sheeran et al. 2002)).

Using film scenarios provides the advantage that the wide spectrum of services can be shown as well as the visualization of services 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. The methodological approach taken here is therefore new. It may be interesting for UC researchers in general, because they have to envision what exactly their applications will look like to future users and can test alternatives in advance. In his way potential acceptance problems may be detected and corrected early in the development cycle.

3.7 Conclusion: Information Collection with RFID

RFID is a mega-trend for the industry. In Germany alone it is expected that RFID will create a value add for the industry totalling about 62 billion Euros by the year 2010. 'Real-time economy' is starting to become a true option due to RFID (Thiesse 2006). And, every product has the potential to be digitally enhanced with it, serving as a key to retrieve personalized information services for our belongings. However, these promises bear one challenge - to embed RFID in our everyday products in such a way that it is accepted by consumers. If RFID is to be used as an enabling technology to create rich information service environments for consumers, then we need to find ways to make this technology safe and relatively free from consumer effort.

According to an online consultation of the European Commission in which 2190 people participated, a majority (68%) felt that RFID application providers should select RFID systems that provide appropriate security and privacy mechanisms. However, fuzzy ideas about what people are afraid of when they talk about privacy don't help. In many circumstances people consciously opt to be tracked and they want their objects to be assessed, for example to increase security. Therefore, the qualitative research we conducted was essential to gain an insight into what precisely it is that consumers fear. Here we found that it is not tracking per-se that they oppose. The qualitative research we conducted suggests that people accept retailers to deploy RFID in their proper premises. In public spaces, however, such scanning is not appreciated. Also, the assessment of objects, as such, is not what people seem to deprecate most. Instead, it seems as if people object to the idea that they may have to sacrifice control over what they own. We explained this through the psychology of ownership (Pierce, Kostova et al. 2002). Against this background, it may well be that people object less to have tagged cloths read-out which they have not bought yet or to have cars scanned which they have just rented for a short term, but do not own.

Finally, information collection for personalization and advertisement are often quoted as a consumer concern in the context of privacy research in general and also with a view to RFID. Yet, it seems that it is not collection and use per-se which people fear. Instead, they question the abuse of this information by collecting entities against their will and the ways the intelligent infrastructure will address them in public space. Many people appreciate personalization practices and individual advertisement (Kobsa 2007), but we question how they would feel about an identical address in public space where others observe the offerings made (for example, offers made by an intelligent shelf display).

The reflection of findings shows that our research has contributed to clarify and detail the more general observations of RFID related consumer concerns published by marketing agencies. Such highly granular analysis allows marketers to tailor RFID practices such that consumers will appreciate them. For example, they could refrain from the use of RFID readers in the semi-public spaces they control, and they may reduce RFID read-outs to the objects they sell and not collect data from the objects people carry when entering a store. They could abstain from classifying people according to their economic potential and instead focus more on cross-selling practices.

Beyond taking such subtle steps to avoid customer annoyance, retailers need to have a deactivation strategy for RFID checkouts. But which one should they adopt? To understand the technical drivers of consumer concerns we conducted an attack-tree analysis. This analysis made plain that beyond organizational measures there really is one main lever to protect peoples' privacy. This is to give them control over RFID tag-reader communication. Already today, approximately 70% of the literature on RFID treats the subject of RFID tag-reader communication. But are engineers on the right track? Do they build the technology with a view to giving people cognitive, decisional and behavioural control over the technology? Our work has contributed to structure and reflect on the strengths and weaknesses of the main directions into which RFID privacy engineers currently work. For this purpose we have been differentiating between the On-tag, User, and Agent Scheme. Delving into the details of current scientific works, however, we find that too many works focus on the pure On-tag protection scheme, excluding the user as a player. At the same time, too few works model the user explicitly as part of the control loop. And those that do are yet in children's shoes. We hope that by creating such clarity about paradigmatic differences in PETs for RFID we are giving some direction to the engineering community on where to focus their efforts. Moreover, we have developed scales to

assist engineers in assessing the value of their technologies from a user perspective. The scales to measure perceived control over the intelligent RFID infrastructure are not only applicable to RFID. They can also be easily adapted to other UC service infrastructures which approach people in a proactive manner.

A major result from our work is that RFID usefulness perceptions may not always outweigh the social cost. 70% of the participants in study ① and 61% in our study ② were clearly in favour of killing RFID tags at store exits rather than using an Agent or User Scheme. And this finding could on average not be attributed to any personal variables of study participants, such as negative attitudes towards new technologies generally or computer anxiety. Also this judgement was not reduced to particularly privacy sensitive participants. In contrast, a large majority of participants in both studies clearly recognized RFID based after-sales service benefits. The reason for this kill preference rather seems to reside in the fact that people do not perceive control over RFID tag-reader communication when confronted with any current RFID PET. Film material was in our view ideal to make participants understand what future PETs would ideally look like (assuming seamless functioning) and how they would interact with the RFID infrastructure. But against expectations the User Scheme, which theoretically implies maximum user control, was perceived as negatively as the Agent Scheme. And this had nothing to do with potential password handling cost either and thus transaction cost. Only 3 out of 108 comments on why one would want to kill RFID chips rather than using a password-based User Scheme related to the hassle or pitfalls of password management. Instead perceived helplessness, vis-à-vis RFID communication streams, ruled peoples' critical judgements of the new technology. Digging deeper into participants perceptions through qualitative analysis revealed that 70% of those who want to kill RFID tags simply distrust the effectiveness of the protection schemes offered.

This work does not provide detailed answers as to how trust building can be actively supported by PETs deployed in intelligent infrastructures. Future researchers should concentrate more on this issue when designing PETs for RFID and other intelligent infrastructures. This work has only highlighted the necessity to tackle this issue, introduced the control requirements, elaborated potential routes to take and provided a first set of potential trust building steps to consider next.

All of the observations and contributions made in this chapter 3 are related – from a bird's eye – to the automation of information collection and acceptance challenges of this potential area of UC. The next chapter will complement to this analysis of the input side of UC by setting a focus on the output side of the new computing landscape. Once information is collected, something needs to be done with it. As the analysis in chapter 2 revealed, few UC applications are yet pro-active in nature. If Ubiquitous Computing wants to live up to its vision of supporting people in the background and act autonomously for them, then more developments are probably expectable. The following chapter will therefore discuss and analyse some major factors for UC engineers to consider in order to create services which are from the beginning appreciated and marketable.

4

A Ubiquitous Computing Acceptance Model and the Role of Control over Automated System Activity

4.1 Technology Acceptance Research and its Transferability to Ubiquitous Computing

Despite a decade of technical research and development in the area of UC as well as high market expectations, very little research exists on factors that will drive the acceptance of the new technological landscape. Computer science scholars tend to view ‘acceptance’ as incrementally linked to the technical parameters of UC systems such as battery life, device interoperability, data management, etc. (Islam and Fayad 2003). However, as these technical challenges are resolved over time – which is a major premise made here – other acceptance factors will come into play. These are concerned with the question of what drives and impedes consumers to adopt the new service landscape once they are technically mature to be marketed. As we have seen above, UC services are to a large extent built to serve people in a private context. This implies that they need to correspond to the expectations and needs of consumer markets. In chapter 3 above it became obvious that the automatic collection of information could create acceptance challenges. Here we focus on the actual service delivery

Past research has shown that people do not mechanically embrace every new technology development and that a lack of knowledge about users’ attitudes toward the use of new technology is one of the major pitfalls when it comes to the diffusion of innovations (Tornatzky and Katherine 1982). The most important dimensions for innovation diffusion according to (Rogers 2003) are minimal complexity of the new product or service, the creation of a relative advantage over existing solutions, and a compatibility with existing norms and values. On a more concrete level, technology acceptance research confirmed two of these dimensions for desktop computing. Looking into the uptake of information systems (IS) applications over the past twenty years, researchers found that the usefulness of a system and its ease of use are determinative for system adoption (Davis, Bagozzi et al. 1989; Davis 1989). Usefulness is conceptually close to relative advantage. And, ease of use relates to the complexity issue potentially hindering innovations’ uptake. The observation that a system’s usefulness and ease of use determine users’ intention to use it as well as actual uptake was termed ‘Technology Acceptance Model’ (TAM). This model has been replicated, validated and extended in more than 140 journal publications (King and He 2006) (for example, (Mathieson 1991; Taylor and Todd 1995; Malhotra and Galletta 1999; Venkatesh 2000; Venkatesh and Davis 2000) and is able to consistently explain some 40 per cent of variance in the uptake of new IS applications (Venkatesh, Morris et al. 2003).

Despite the widespread embracing of TAM to explain system use, we must question whether it is a good starting point to anticipate and explain the adoption of UC services, and, in particular, of those proactive and privately operated UC services in which we are interested here. Indeed we doubt this for several reasons:

First, TAM has been developed to test IS adoption in professional environments. As a consequence, personal attitudes towards systems were early omitted from the model observing that in a professional context peoples' attitudes seem to be less determinative for system adoption (Davis, Bagozzi et al. 1989). Instead, it was shown that the voluntariness of system use in a firm is playing an influential role: if system use is mandated by management then people expect that non-use could impact their performance in an organisation which again makes them (grudgingly?) accept the system (Venkatesh and Davis 2000; Venkatesh, Morris et al. 2003). These dynamics we believe are not transferable to many UC systems. Instead, and as was shown above, we are dealing here with a system landscape that heavily relies on peoples' voluntary embracing of technology, embracing to an extent even that they or their service provider will purchase the technology. Consequently, we expect that personal attitudes towards UC services will gain in relevance. Research in affective attitude and its role for system acceptance has seen a renaissance over past years in the IS world generally (Zhang and Li 2005). Emotional design (Norman 2004) has become a new buzzword for product design. However, as (Yang and Yoo 2004) pointed out, TAM research lacks a proper distinction of even the most rudimentary dimensions of attitude which is to separate affective attitude from its cognitive counterpart. The next section will provide more in-depth reasoning on this issue.

We also believe that TAM lacks the dimension of 'compatibility', which was identified as important for innovation diffusion. Compatibility has been defined as the degree to which an innovation is perceived as consistent with existing values, past experiences, and needs of potential adopters (Rogers 2003). UC system characteristics such as their potential to undermine privacy and control are falling into this category.

TAM should also be limited because it consists of only two main drivers for system adoption: usefulness and ease of use. While usefulness is certainly an argument for UC services (as we will show below), ease-of use is probably less so. Ease of use is defined as "the degree to which a person believes that using a particular system would be free of effort" (p. 320 in (Davis 1989)). Yet, in UC environments autonomous or "calm" (Weiser and Brown 1996) actions of systems imply a supposed little need for user interaction. Assuming that systems work properly and invisibly in the background, specific skills or learning should not to be required any more. An example from automation history may clarify this argument: while originally the starting motor of an automobile was manually operated requiring physical skill and strength, automobiles present no such challenge today as they are started automatically upon key insertion or even without that, using keyless-to-go technology. Assuming that engineers will succeed in designing UC services along these lines, we expect that there will therefore be minimal influence of ease of use perceptions on the judgement of a system's usefulness, the intention to use it or differential attitudes towards the system. Consequently, TAM would be deprived of one of its two explanatory dimensions, which renders the model too parsimonious to remain useful. This reasoning assumes, of course, that engineers have mastered the challenge of building systems which seamlessly adjust to users; a task, we acknowledge to be of utmost difficulty.

Finally, TAM's dependent variable has always been peoples' intention to use a system. While use intentions are key to reflect system acceptance they may not be enough to predict market success. Therefore it is equally important to measure whether people would want to buy a respective service.

Given these arguments, we have opted to not expand on the traditional TAM, but instead develop a new acceptance model from scratch, the UC Acceptance Model, UC-AM.

4.2 Conceptual Framework for a Ubiquitous Computing Acceptance Model

In constructing the UC-AM we draw from several major research streams, notably from the field of social psychology (Fishbein and Ajzen 1975), management information systems (Davis 1989), environmental psychology (Mehrabian and Russell 1974), engineering (Sheridan 2002), and affective computing (Zhang and Li 2005). Based on these diverse sources spanning across disciplines, we deduce and combine major constructs and relationships which we expect to be important for explaining future UC acceptance. In this way we successively build a hypothetical model of acceptance of UC services which we then test empirically. The central focus is to explain the intention to use or buy a proactive UC service in the private realm.

4.2.1 Hypotheses on the Drivers and Impediments of UC Acceptance

4.2.1.1 *The role of cognitive and affective attitudes for UC acceptance*

Traditionally, the intention to do something (anything!) is explained by social psychologists by the means of attitudes. The attitude a person holds about a certain behavior is defined as “an individual’s positive or negative feelings about performing the target behavior.” (p.216 in (Fishbein and Ajzen 1975)). Empirical work and meta-studies in the context of the Theory of Reasoned Action (Fishbein and Ajzen 1975) (Sheppard, Hartwick et al. 1988) and the Theory of Planned Behavior (Ajzen 1985) have proven that attitudes correlate highly with behavioural intentions (correlations ranging from .45 to .69 (see (Ajzen 1991) p. 196) which then drive action (mean correlations of .53 according to (Sheeran 2002)). Therefore, attitude formation is at the centre of the UC acceptance model proposed hereafter.

Consensus has been achieved on the distinction of cognitive and affective attitude (Petty, Wegener et al. 1998). Cognitive attitude refers to an individual’s specific evaluative belief that “it is to [one’s] advantage or disadvantage to perform the behavior” (p. 380 in (Trafimow and Sheeran 1998)). Cognitive attitude is characterized by adjectives such as wise/foolish or beneficial/harmful (Crites, Fabrigar et al. 1994). Affective attitude, in contrast, refers to how much a person likes an object of thought or “how [she] feels about performing the behavior” (p. 380 in (Trafimow and Sheeran 1998)) Attitude in this sense is considered an instance of affect, often equated and measured in the same way as emotion (Bagozzi, Gopinath et al. 1999). It is characterized by word pairs such as delighted/sad, happy/annoyed or like/dislike (Crites, Fabrigar et al. 1994).

(Yang and Yoo 2004) criticise that TAM researchers have regularly neglected or even mixed the different dimensions of attitude despite their potentially distinct influence on IT adoption. (Yang and Yoo 2004) found that primarily a person’s cognitive attitude towards a system determines the use of spreadsheet applications. In line with this finding we hypothesize:

H1: The more positive a person’s cognitive attitude is towards a system the higher is the intention to use it and buy it.

In 2007 Apple Inc. introduced its new combined cell phone, the iPhone, which simultaneously functions as iPod, e-mail client and Internet appliance. The product launch was feverishly anticipated by thousands of customers, putting up with hours of waiting times in front of stores. One customer exclaimed: "I took my new jewel to a dinner party last night. Everyone was all over it. Everyone loved it. The host broke out champagne, and we all toasted to it."³² This quote shows the potential that new devices and their services can stir strong affective reactions. Interesting enough none of these people queuing can ever have had the possibility to directly interact with the device in advance. Only the expectation of pleasure led people to buy the phone right away.

(Zhang 2005) argues that affective reactions to IS objects drive the intention to use them as well as actual usage. In order to understand the role of affect in IS (Zhang 2005) conducted a meta-study on affect related IS research. She found that indirectly through constructs such as flow (Csikzentmihalyi 1990; Koufaris 2002), computer anxiety (Compeau and Higgins 1995) or computer playfulness (Hackbarth, Grover et al. 2003) affective attitude has for long been a subject for IS scholars. Moreover, affective factors are increasingly being recognized in the usability community as a crucial factor influencing the user experience. Tractinsky found that people evaluated an aesthetically pleasing ATM-machine as more usable despite offering exactly the same functions as the less pleasing ATM-machine (Tractinsky, Katz et al. 2000). (Hassenzahl 2001) emphasizes the role of hedonic qualities of user interfaces for users' willingness to interact. As a result, we expect that UC engineers may need to embrace more of the insights gained on "emotional design" which has been recognized as essential for technical product take-up in consumer markets (Norman 2004). We do so even though traditional TAM scholars (Yang and Yoo 2004) could not confirm affective attitude as a relevant driver for system adoption. As was outlined above, this may be due to the fact that behavior in professional environments is more driven by performance expectations than the desire to have fun (Davis, Bagozzi et al. 1989; Venkatesh, Morris et al. 2003). Yet, since a majority of UC services will be used in the private realm system adoption will be mostly voluntary and needs to appeal to users. We therefore hypothesize:

H2: The more positive a person's affective attitude is towards a system the higher is the intention to use it and buy it.

By integrating affective attitude as a generalized construct into our model, we argue that emotions like computer anxiety can indirectly be at play, as could be surprise and diversion (Gaver and Martin 2000), beauty (Alben 1996) or intimacy (Vetere, Gibbs et al. 2005). For reasons of parsimony, however, we treat affect (just as cognition) as conceptual 'chunks' the drivers of which can be researched in separate efforts. Furthermore, it is easier for people to imagine global affective reactions to a given scenario than to evaluate specific emotional epiphenomena (Loewenstein and Schkade 1999).

Whether affective attitudes are more important for using a proactive UC system than cognitive ones (or vice versa) is unclear. Some researchers in traditional IS have pointed out that the two concepts are interrelated and evidence for mutual influence is mixed (Zhang 2005). For the current work, it has not been a focus to hypothesize any particular direction of influence. Instead we are interested in those factors, which influence attitude formation in UC environments. The following sections will lay the scientific grounds and reasoning for including usefulness, privacy, control, and risk beliefs as key drivers for attitude formation.

³² "iPhone reactions range from glee to: 'Anyone want to buy my iBrick?'" retrieved from: http://www.twincities.com/ci_6287781 (last reviewed on August 20th 2007)

4.2.1.2 The importance of usefulness of Ubiquitous Computing services

A starting model for technology acceptance research has typically been the TAM as proposed by (Davis, Bagozzi et al. 1989; Venkatesh 2000; Venkatesh and Davis 2000). As was outlined above, it postulates that perceived usefulness (USF) of an IS and its ease of use (EOU) are the only main determinants for the intention to use a system as well as usage behavior. USF is defined as “the degree to which a person believes that using a particular system will enhance his or her job performance” (p. 320 in (Davis 1989)).

Even though USF of IT was originally related to job performance, evidence exists that it is equally applicable to the less performance driven private realm (Straub, Limayem et al. 1995; Henderson and Divett 2003). One reason for the broad applicability of the usefulness construct is that it roots in expectancy-valence theory (Vroom 1964). If people value the outcome of system adoption (as is implicated by the term ‘useful’) then they are willing to embrace it. Thus usefulness does not need to be related solely to performance on the job (as (Venkatesh, Morris et al. 2003) suggest). Therefore we hypothesize:

H3: The more useful a UC service is perceived to be, the more will a person intend to use it and purchase it.

(Yang and Yoo 2004) equally show that cognitive attitude is mainly driven by usefulness perceptions. In line with their findings we hypothesize:

H4: The more useful a system is perceived to be, the better is a person’s cognitive attitude towards its use and purchase.

4.2.1.3 The role of privacy for pro-active UC systems

Maintaining privacy has been echoed by a majority of UC researchers as one of the major challenges for UC acceptance (Jessup and Robey 2002; Bohn, Coroama et al. 2004; Lahlou, Langheinrich et al. 2005) and in chapters 2 and 3 above we have expanded on this issue. The reason for discussing privacy issues in UC is that the services foresee information about users to be constantly, ubiquitously and automatically collected and used to create context relevant profiles. Based on these user profiles, systems are supposed to react intelligently to people. For example, a smart fridge would analyse its content, deduce consumer consumption preferences and purchase patterns. With this information it would autonomously replenish or make suggestions. When supporting the purchase process it could share its owner’s shopping list and identification data with a retailer. This regular collecting of personal information, its storing, processing and sharing can impact peoples’ privacy.

The relatively young research stream on the ‘economics of privacy’ (Varian 1996; Acquisti, Friedman et al. 2006) would suggest that people carefully weigh the pros and cons of data revelation and use a cognitive rationale to form an attitude towards a service. For example, they argue that hyperbolic discounting is at work when people decide to reveal personal data in order to receive immediate gratifications in return (and discounting future drawbacks) (Acquisti 2004). IS research suggests that people process information cues about companies’ privacy policies and, based on this information, decide to interact more or less with a service (Hui, Teo et al. 2007). Because we have seen that scholars believe in such cost-benefit rationale being at work when people decide to reveal data, we hypothesize that privacy concerns must have some impact on cognitive attitude:

H5: The more privacy concerns a person has with regards to using a UC service, the more will he or she will hold a negative cognitive attitude towards the service.

However, past years of research in the privacy field have equally shown that people in many cases do not seem to act in accordance with the privacy concerns they voice over service usage (Spiekermann, Grossklags et al. 2001; Berendt, Guenther et al. 2005). They reveal data in many more cases than they say they'd do. Some of this behavior may go beyond the cognitive rationale suggested by privacy economics scholars. For example, (Westin 1967) describes a link between privacy and affect by pointing to the 'emotional release' function of privacy. Here privacy relates to peoples' desire (and pleasure?) to be free from playing several distinct role(s) in society (Goffman 1959). A different piece of evidence on the affective side of privacy behavior and perception is described by (Huberman, Adar et al. 2004). They show that when a person's personal information diverges from their group's mean this person feels less comfortable to reveal it. Such discomfort could be reflected in a negative affective attitude towards systems which force them to reveal. Against this background we hypothesize:

H6: The more privacy concerns a person has with regards to using a UC service, the more will he or she hold a negative affective attitude towards the service.

Finally, the question arises whether privacy concerns could also directly impact the intention to use a system. Sociologist (Altman 1975) views privacy behavior as a constantly ongoing "interpersonal boundary-control process, which paces and regulates interaction with others" (p.10). Is attitude construction a systematic part of this control process? We argue that this may not necessarily always be the case. An example may illustrate this: Assuming that we own cars which embed an automated maintenance system which schedules repairs when needed. By doing so it conveys the entire condition of the car in detail to the nearest garage. Some car drivers could feel that this is too much information revealed. They may consider the maintenance functionality as generally sensible and beneficial leading to a per-se positive cognitive attitude towards the system. They may also like the system and feel safer due to its existence. But they still do not want the data transfer to happen. In such a case it is not the attitude that counts. Instead the concern over privacy could directly drive the intention not to use the UC system. The fact that some people are fundamentally concerned to guard their privacy - and that this is the case regardless of the system under scrutiny - has been shown in myriad empirical user studies (Ackerman, Cranor et al. 1999; Spiekermann, Grossklags et al. 2001; Acquisti and Grossklags 2005). Against this background we add a third privacy related hypothesis to our model:

H7: The more privacy concerns a person has with regards to using a UC service, the less will she intend to use it or buy it.

4.2.1.4 About the role of perceived control for UC evaluation

When Mark Weiser conceived his vision of UC in terms of calm and autonomous systems working in the background he anticipated that "...the problem [associated with UC], while often couched in terms of privacy, is really one of control" (p.694 in (Weiser, Gold et al. 1999)). Indeed, as has been outlined above, Weiser hinted to a challenge that has for long been observed and debated in other fields of engineering and computer science where systems have taken over human tasks, act largely autonomously and often proactively. For example, the development of automated systems in air traffic have seen a history of debates between pilots and airlines as to the optimal 'allocation of functions' between human operators and the automated glass cockpit (Sheridan 2000). Equally, researchers in the area of user-adaptive systems and software agents have continued to discuss the "pros and cons of controllability" (Jameson and Schwarzkopf 2002). People strive for control to maintain psychological well-being (White 1959; deCharms 1968; Langer 1983) and tend to feel helpless if they are repeatedly and notoriously deprived of it (Seligman 1975). Against this background, peoples' control over

proactive UC services may be quite influential for their affective reaction to them. As (Te'eni, Carey et al. 2007) have pointed out: "Users do not want to feel that the machine has taken over (p. 209)."

It should be noted that the type of control referred to in the adaptive systems and automation literature is distinct from the construct of Perceived Behavioural Control as conceived of by (Ajzen 1985; Ajzen 1991). Perceived Behavioural Control adopted largely in the traditional TAM literature resides on beliefs of self-efficacy (Bandura 1977) and access to facilitating conditions (Triandis 1977) (Taylor and Todd 1995; Ajzen 2002). It looks into how good one thinks one can perform a behaviour, given internal and external constraints. When it comes to automated systems, however, the challenge is that users largely do not perform the behavior themselves anymore. Instead machines act for them. When dealing with perceptions of control vis-à-vis pro-active services, the construct can therefore be better captured by the notion of power balance with and choice over machine actions, the personal perception to be informed about what is going on ("situation awareness" (Endsley 1996)) and the right to have a last say over a machine's processes if needed (Spiekermann and Pallas 2005). Langer's definition of control may be quite suited to capture this understanding of the construct. She defines control as "...the active belief that one has a choice among responses that are differentially effective in achieving the desired outcome... the mindful process of mastering" (p.20 in (Langer 1983)). In this sense control over UC environments resembles "access to functions". Access to functions is described as a fundamental characteristic of assistance systems by (Wandke 2005). It is a prerequisite for a notion of perceived control which was introduced extensively as a concept in section 2.3.2.1 above.

When objects start to act autonomously and proactively trigger actions, people may easily perceive themselves to be out of the loop. This leads to negative affective attitudes (Ward and Barnes 2001). In one qualitative study by (Ringbauer and Hofvenschiöld 2004) the researchers showed that subjective feelings of a loss of control were a primary impediment to smart home acceptance. Another study by (Rijsdijk and Hultink 2003) showed that the degree of autonomy of three domestic UC products would add to users' perceived product risk and by that indirectly influence product appreciation in a negative way. On the basis of these findings we hypothesize:

H8: The lower the level of perceived control over a system, the more negative will be the affective attitude of a person towards using or purchasing it.

Furthermore we expect users' perceived control over a system to directly influence the behavioural intention to use it. We base this hypothesis on two streams of research: One is reactance theory (Brehm 1966). Reactance describes a "condition under which people will react against attempts to control their behavior and eliminate their freedom of choice (p. 390 in (Clee and Wicklund 1980))." This reaction is intuitive and negative and marked by the desire to move into exactly the opposite direction than the controlling force tries to impose. Some researchers have described reactance arousal as "hostility toward the agent who has threatened the behavioural freedom" (p.109 in (Brehm 1966)). When machines start to act autonomously and proactively, some potential exists that people will experience this type of negative arousal perceiving that their choice set and freedom is reduced, in particular, when 'the last word' to kick-off a process is with the machine and not with the human being (as is the case in the UC service landscape investigated below). Furthermore, findings from environmental psychology (Mehrabian and Russell 1974) suggest that approach and avoidance behavior directly depends on the degree of dominance, one feels vis-à-vis an environment. The dominance construct is defined and measured in the same way as control in terms of freedom of choice and therefore often used interchangeably (Hui and Bateson 1991; Ward and Barnes 2001). Both reactance and approach/avoidance behavior have been described as intuitive reactions to the environment and independent of attitudes towards that environment. Therefore, we hypothesize:

H9: The lower the level of perceived control over a system, the lower will be a person's intention to use or purchase a given system.

4.2.1.5 *Perceived risk as a cause of UC rejection*

Some scholars have recently pointed to the potential role of risk perceptions for IS adoption (Spiekermann 2001; Featherman and Pavlou 2003; Spiekermann, Strobel et al. 2005; Krasnova, Rothensee et al. 2007). Perceived product risk is defined as “the expectation of losses associated with a purchase” (p. 185 in (Peter and Ryan 1976)). In marketing theory it is considered a key construct relevant for the formation of attitudes towards purchasing a product or service (Bauer 1960). As we want to understand attitude formation for the use of UC services, risk could therefore be a relevant factor. UC implies that many of today’s ordinary objects are going to be enhanced with computing power and will integrate information services as well as reactions to users. As a result, consumers will reflect on the risks associated with the new UC services embedded in the products they evaluate for use. (Featherman and Pavlou 2003) could show that consumer perceptions of risk reduce their beliefs of the usefulness of services as well as their intent to use them. A similar finding was presented by (Rijsdijk and Hultink 2003) who found that consumer appreciation of three distinct autonomous products was mediated by the perceived performance risk associated with a product. And finally (Wu and Wang 2005) could provide evidence that in the context of mobile commerce perceived risk impacts the behavioural intention to adopt the new channel. Against the background of these findings we hypothesize:

H10: The more risk a person perceives associated with a UC service, the less she intends to use or purchase it.

Researchers have shown that consumers perceive multiple types of risks when searching for and purchasing a product including financial, psychological, physical, functional, social and time risk (Cunningham 1967; Kaplan, J. et al. 1974). Financial risk is the risk that a product will not be worth its financial price. Financial risk could be created by additional procurement and maintenance cost of a UC system or unwanted autonomous actions by the system, such as smart fridge procuring overpriced goods. Psychological risk is the risk that a poor product choice will not fit with a consumer’s ego or day-to-day life style. For example, people may enjoy doing things which are substituted by intelligent systems. A smart fridge would thus not fit in with a person’s daily shopping trips if he or she loves shopping. Physical risk is relatively rare today. It is described as the risk to a buyer’s or other’s safety in using a product. If UC services are misconfigured, it cannot be excluded that they cause harm. Functional risk in contrast is defined as the systematic risk that the product will not perform as expected. This risk may be particularly important in a world of proactive UC services if UC enabled products do not act in line with what their owners want. Social risk means that a product choice could cause embarrassment before ones friends, family or work group. Whether social risk will be as relevant to judge UC services as it is to individual products is questionable. While some products (such as cloths) come in many variants and are subject to different tastes and fashions, UC services will probably come in standardized form. Therefore, the anchor for peer judgements may be less prevalent. Finally, time risk stands for the possibility that through using the product or service one may lose time. Indeed, it could be that UC services bear this risk. Even though proactivity suggests that people will save time a possibility remains that systems take more time than what users would need.

(Cunningham 1967; Featherman and Pavlou 2003) have shown that the diverse risk facets share a common core, so that it is possible to unify risk perceptions under the umbrella of an overall risk assessment. The diverse types of risk could imply that some of them are more related to the instrumentality of a product or service (i.e. the functional risk) while others are closer to the emotional well-being of a person (i.e. psychological risk). In light of the exploratory nature of our work, however it seems unwarranted to hypothesize specific relationships between risk components and other acceptance related constructs. Therefore we decided to employ a unified risk measure, overall perceived risk (ORP). We expect that both cognitive and affective attitudes will be influenced by a combined measure. Therefore, we include two further hypotheses in our model of UC adoption, which are to test the distinct impact of risk on cognitive and affective attitude:

H11: The more risk a person associates with a UC system, the more negative will be his or her cognitive attitude towards the system.

H12: The more risk a person associates with a UC system, the more negative will be his or her affective attitude towards the system.

Figure 22 visualizes the hypothetical UC-AM resulting from the expected relationships between these constructs.

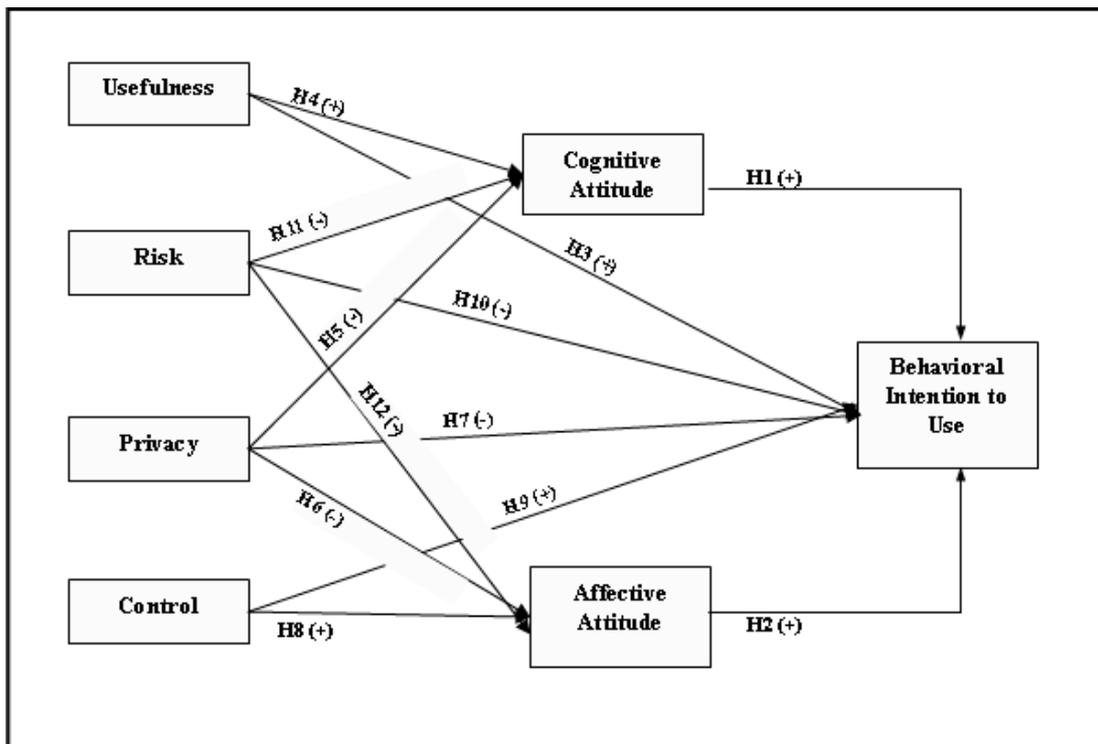


Figure 22: UC Service Acceptance Model– Hypotheses and (expected directions)

4.2.2 Method to Investigate the UC-Acceptance Model

4.2.2.1 Development of the stimulus: UC scenarios tested

Testing UC services presents a challenge to research as long as there are few such services deployed. Furthermore, UC services are so pervasive that it is desirable to develop models with predictive power across a wider range of applications instead of just one service or device. We therefore opted to test the same hypotheses for three UC services from different contexts. We presented the three service scenarios to subjects with the help of a short description as well as two accompanying graphics produced professionally and exclusively for the study (appendix 4). The scenarios were presented through an online questionnaire. They related to an intelligent fridge which autonomously places orders, an intelligent speed adaptation system (ISA) which brakes the car automatically when the

route's speed limit is passed, and a car that services itself and schedules a meeting with a garage if parts are about to wear out. Figure 23 presents one of the three scenarios describing the ISA system.

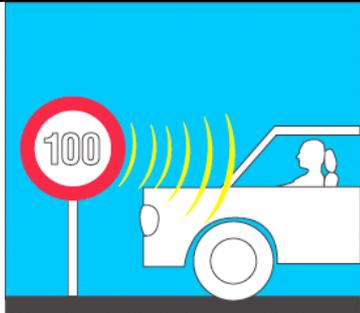
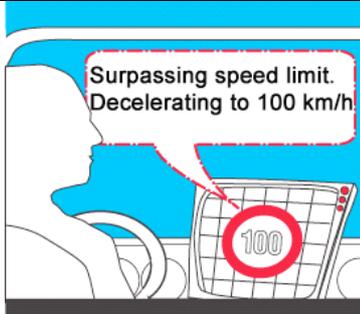
Intelligent Speed Adaptation (ISA)	
<p>It is the year 2015...</p> <p>My car has become intelligent by the help of numerous sensors. The intelligent functions above all are meant to increase my safety. One of these intelligent functions is the automatic speed limit. This function is an obligatory legal regulation to all cars, except for police, ambulance and fire brigade.</p> <p>The system works such that speed limit signs send radio signals to my car, transmitting the required speed limit to it. [high control scenario : If I am driving too fast, my car automatically notices this violation. The navigation system recommends me to brake in order to stay within the speed limit. / low control scenario : If I am driving too fast, my car automatically decelerates. The navigation system informs me that it has automatically decelerated in order to stay within the speed limit.]</p>	
	<p>The Intelligent Speed Adaptation System</p> <p><i>What the system looks like</i></p>
	<p><i>What the controls look like:</i></p> <p>Low control</p>

Figure 23: Scenario description of the ISA system displayed to study participants

In one criterion for choosing these three contexts, we wanted scenarios which easily emanate from subjects' current experiences limiting the degree of imagination necessary. Furthermore, we deliberately focused on devices that are well-researched in the industry in order to make our results more realistic and interesting for the scientific community (Vlacic 2001; Várhelyi 2002; Klamer 2005). In another criterion for choosing the scenarios we wanted to include services which elate to privately owned objects, but are apt to private as well as public dynamics (home vs. street). We do this because both privacy and control have been shown to be impacted by the territories in which they are exercised (Goffman 1959; Altman 1975).

In the scenario text, we implied ownership of the product in all scenario wordings, because it has been shown that this aspect influences interaction with objects (Pierce, Kostova et al. 2002). Two types of control were implicated in the way the scenarios were described: first, control over the immediate UC

service integrated in the product as a function (behavioural control) and second, control over the UC service provider (decisional control). We ensured that all scenarios would equally provide the user with decisional control over the UC service provider (e.g. the garage where the car will be maintained or the shop where food will be ordered). At the same time we manipulated the degree of behavioural control over the system's functionality: In all three scenarios it corresponded to level six specified in Sheridan's model of operator control (Sheridan 2002). This level specifies: "[The computer] executes automatically, then necessarily informs the human" (p. 62 in (Sheridan 2002) and table 3).

Based on a focus group with 7 participants and 5 individual interviews we continuously revised the scenario descriptions. Here it turned out that people would generally want to understand the motivation of the new service (e.g. safety). Also, exception handling (e.g. an emergency case) would be important and the choice over the UC service provider.

Following this first revision cycle a laboratory study with 8 participants was conducted to test texts and graphics of the online questionnaire as well as their interplay. Graphics were edited to ensure neutral appearance. Finally, the full stimulus was tested with 52 participants in an online pre-study to understand whether it would be comprehensive and trigger sufficient variance in answering behavior. Appendix 5 gives an overview of the steps involved to prepare the study.

4.2.2.2 Setting and data collection procedure

After this extensive pre-testing the scenario descriptions were posted on the Internet alongside an online questionnaire for four weeks in January 2007. Participants were informed about the study through handouts distributed on the campus of Humboldt University Berlin. They were invited to participate in evaluating "tomorrow's technologies" in exchange for a fixed sum of € 5 and additional participation in a lottery offering an Apple iPod. To participate in the study they would need to access the online survey independently via the link indicated to them on the handout.

266 persons fully completed the questionnaire for the UC scenarios. Participants were nearly equally female (53.6%) and male (46.4%), most of them were well educated (61.3% graduated from high school) and regular PC users (62.1% almost exclusively/completely work using computers). 84.3% were below 29 years of age, 13.5% between 30 and 49 years and 2.2% older than 49. On average, it took participants 37 minutes to complete the questionnaire. The order in which participants saw the scenarios was varied by chance to avoid order effects.

4.2.2.3 Instruments

Construct measurement was done in line with earlier research (questionnaire and item definitions are included in appendix 7). Three items testing perceived ease of use and USF were taken from (Davis 1989) and adjusted to the private setting by emitting the reference to 'jobs'.

An overall perceived risk index (OPR) was measured with a view to marketing theory where two risk components are distinguished in the context of purchase decisions: "...a chance aspect where the focus is on probability [of losing] and a 'danger' aspect where the emphasis is on severity of negative consequences of purchase" (Cunningham 1967; Peter and Tarpey 1975). Based on the arguments presented above, four risk dimensions have been recognized: the functional, financial, psychological and time risk. For each of these dimensions the two components of risk were measured, multiplied and then added up to form an OPR index.

Attitudes are often measured with the help of semantic differential items. We employed a 9-point scale for three items measuring the affective attitude towards a service analogous to (Mehrabian and Russell 1974) and three items measuring cognitive attitude analogues to (Crites, Fabrigar et al. 1994; Yang and Yoo 2004).

A four-item scale was developed to measure potential privacy concerns in conjunction with the respective services. In line with (Smith, Milberg et al. 1996; Spiekermann and Cranor 2007) several

aspects of privacy concerns were covered by these items, including information collection, transfer and secondary use (including the sharing of data with unknown 3rd parties).

A two-item control scale was self-developed on the basis of the definition proposed by (Langer 1983).

In order to measure behavioural intention to use, we developed a scale based on the work of (Mick and Fournier 1998). The authors have investigated consumer strategies to cope with new technologies (e.g. video recorders, answering machines, etc.). In particular they identified two main after-purchase use strategies: (1) Avoidance strategies leading to neglect, abandonment or distancing from the technology bought and (2) Confrontive strategies leading to an accommodation with, partnering or mastering of technology. Based on this insight, we developed and tested three items for abandonment, partnering and mastering respectively that would form one factor to measure the intention to use a technology.

Finally, we measured the subjects' willingness to buy with two items. We did so however exclusively for the intelligent fridge scenario. This is, because the car scenarios are of semi-public nature and services introduced in this context may in the scenario text be considered as less apt to private decision making. The ISA system was directly described as mandatory to participants. Annex 7 contains the questionnaire with items used.

4.2.3 Results: Fit and Strength of the UC-Acceptance Model

4.2.3.1 Test of measurement models

Importantly, we were challenged to prove that the hypotheses equally hold true for all UC scenarios. Consequently, we needed to prove the existence of our constructs as well as highly similar relationships between them across scenarios and for both use and purchase decisions.

We did so by first assessing the constructs' internal consistency as well as discriminant validity for each scenario. Furthermore we used the structural equation modelling technique Partial Least Squares (PLS) to subsequently test our hypotheses. PLS is a procedure well suited for predictive analysis (Chin 1998) and has been used extensively in IS research. PLS modelling was realized with the software SmartPLS (Ringle, Wende et al. 2005).

Construct validity was assessed through the outer loadings generated through the PLS procedure. In a PLS structural model, the outer loadings of indicators on the corresponding constructs can be interpreted as loadings in a principal components factor analysis. Table 17 shows that only 5 of the outer loadings of the 75 indicators are slightly below .70 (which is the quality index level that should typically be reached by factor loadings, p.325 in (Chin 1998)) and that these are dispersed across scenarios and constructs. We therefore argue that the constructs have a sufficient validity in all scenarios. Furthermore, Cronbach- α values summarized in tables 18 to 21 show that constructs show a high internal consistency. Cronbach Alpha indices are continuously above the 0.70 threshold, mostly even above 0.80. To control for conceptual proximity between the constructs we furthermore examined the discriminant validity of our measures for every scenario using the square root of the average variance extracted (Fornell and Larcker 1981). As shown in tables 18 to 21 square roots of the average variance extracted are greater than the off-diagonal construct correlations in the corresponding rows and columns. This implies that no matter what UC scenario, each construct shares more variance with its items than it shares with the other model constructs.

Table 17: Outer loadings of indicators on the UC - AM constructs

Constructs	Indicators	ISA	Fridge (Use)	Fridge (Buy)	Garage
CogATT	KA1R	0,910	0,899	0,899	0,940
	KA2R	0,906	0,883	0,884	0,933
	KA3R	0,954	0,899	0,898	0,948
CTRL	KTR1R	0,819	0,923	0,924	0,926
	KTR2R	0,895	0,938	0,937	0,946
	OPR	1,000	1,000	0,904	1,000
AffATT	PADP1	0,924	0,903	0,904	0,931
	PADP2	0,927	0,912	0,911	0,897
	PADP3	0,930	0,904	0,904	0,927
PrivConc	PRIV1/2R	0,641	0,775	0,774	0,733
	PRIV5R	0,731	0,789	0,783	0,815
	PRIV6R	0,726	0,613	0,613	0,678
	PRIV7R	0,814	0,806	0,810	0,763
USF	USE1R	0,772	0,862	0,860	0,841
	USE2R	0,830	0,779	0,778	0,815
	USE3R	0,890	0,895	0,897	0,899
BI	VNK1	0,901	0,875	0,934 (VVK1R)	0,879
	VNK3R	0,881	0,878	0,929 (VVK2)	0,878
	VNK4R	0,583	0,743	-	0,704

Table 18: Discriminant validity of measures scenario 1: intelligent fridge (intention to use)

	Cron Alpha	AffATT	BI	CTRL	CogATT	OPR	PrivConc	USF
AffATT	0,89	0,91						
BI	0,78	0,67	0,83					
CTRL	0,85	0,59	0,57	0,93				
CogATT	0,87	0,75	0,65	0,58	0,89			
OPR	1,00	-0,46	-0,46	-0,45	-0,46	n.a.		
PrivConc	0,74	-0,34	-0,33	-0,43	-0,28	0,34	0,75	
USF	0,80	0,70	0,71	0,63	0,78	-0,50	-0,31	0,85

*Note: AffAtt= affective attitude, BI = behavioural intention to use, CTRL = control, CogAtt = cognitive attitude, OPR = overall perceived risk, PrivConc = privacy concerns, USF = usefulness

Table 19: Discriminant validity of measures scenario 1: intelligent fridge (intention to buy)

	Cron Alpha	AffATT	BI	CTRL	CogATT	OPR	PrivConc	USF
AffATT	0,89	0,91						
BI	0,85	0,70	0,93					
CTRL	0,85	0,59	0,69	0,93				
CogATT	0,87	0,75	0,70	0,57	0,89			
OPR	1,00	-0,46	-0,53	-0,45	-0,46	n.a.		
PrivConc	0,74	-0,34	-0,34	-0,44	-0,28	0,35	0,75	
USF	0,80	0,70	0,78	0,63	0,78	-0,50	-0,32	0,85

Table 20: Discriminant validity of measures scenario 2: ISA

	Cron Alpha	AffATT	BI	CTRL	CogATT	OPR	PrivConc	USF
AffATT	0,92	0,93						
BI	0,72	0,75	0,80					
CTRL	0,65	0,56	0,62	0,86				
CogATT	0,91	0,70	0,67	0,46	0,92			
OPR	Index	-0,41	-0,42	-0,45	-0,42	n.a.		
Privacy	0,72	-0,30	-0,34	-0,31	-0,28	0,48	0,73	
USF	0,78	0,67	0,71	0,57	0,77	-0,44	-0,32	0,83

Table 21: Discriminant validity of measures scenario 3: automatic garage service

	Cron Alpha	AffATT	BI	CTRL	CogATT	OPR	PrivConc	USF
AffATT	0,91	0,92						
BI	0,76	0,69	0,82					
CTRL	0,86	0,46	0,56	0,94				
CogATT	0,93	0,80	0,74	0,45	0,94			
OPR	index	-0,49	-0,50	-0,56	-0,52	n.a.		
PrivConc	0,74	-0,33	-0,35	-0,30	-0,24	0,33	0,75	
USF	0,82	0,67	0,74	0,53	0,75	-0,48	-0,27	0,85

4.2.3.2 Testing the UC Acceptance Model for use intentions

Based on the theoretical discussion above, we tested whether the relationships hypothesized are holding true and in particular whether they hold equally true across scenarios. Figure 24 gives an overview of the path coefficients between constructs and their level of significance. The results show that there are indeed stable similarities between the judgements of all scenarios: First, (confirming hypothesis 3) usefulness is a stable driver for the intention to use a UC service and is equally a very strong determinant for a person's cognitive attitude towards it (confirming hypothesis 4). There is no hierarchy of effects though, because against expectations cognitive attitude is not a stable driver of the intention to use as system. In the speed adaptation and fridge scenarios, for example, path coefficients are surprisingly low and insignificant (disconfirming hypothesis 1). Only in the garage scenario cognitive attitude is significant for use intentions. At the same time the data suggests that affective attitude plays an important role for all private UC services investigated (confirming hypothesis 2). Thus for privately owned devices affective service judgement is regularly influential for the adoption intention.

If affective attitude is continuously important for judging UC services, then an important question is what its drivers are. We hypothesized that privacy concerns, perceived risk and perceived control over a service would impact the affective reaction to it. In fact, throughout all three scenarios, perceived control and OPR are significant drivers of the affective attitude towards service use (confirming hypotheses 8 and 12). For the two constructs the data suggests that affect is mediating use intentions. At the same time, privacy perceptions are continuously less influential than expected. Only in the garage scenario privacy concerns exercise a small but significant influence on the affective attitude towards a service as well as a direct negative intention to use. Besides this one observation, no direct influence of privacy concerns exist on behavioural intention, cognitive attitude or affective attitude. Hypothesis 5 must therefore be denied while hypotheses 6 and 7 can only be confirmed for the garage scenario. Equally contradicting earlier findings by (Rijsdijk and Hultink 2003) none of the scenarios confirms a direct relationship between OPR and behavioural intention (disconfirming hypothesis 10).

Finally, mixed evidence exists for the control construct. Even though perceptions of control strongly influence affective attitude formation (confirming hypothesis 8), its direct influence on the intention to use a service is mixed. The more control one perceives, the more is he or she willing to delegate operations to the car; but, in the fridge scenario this relationship is less evident (mixed evidence on hypothesis 9). It is noteworthy that the impact of control perceptions is much stronger on emotions than on use intentions directly. This suggests a hierarchy of effects for control perceptions being channelled through affect. Figure 24 gives an overview of the relationships found. Appendix 6 contains screenshots of the individual structural equation models as the have been generated by PLS.

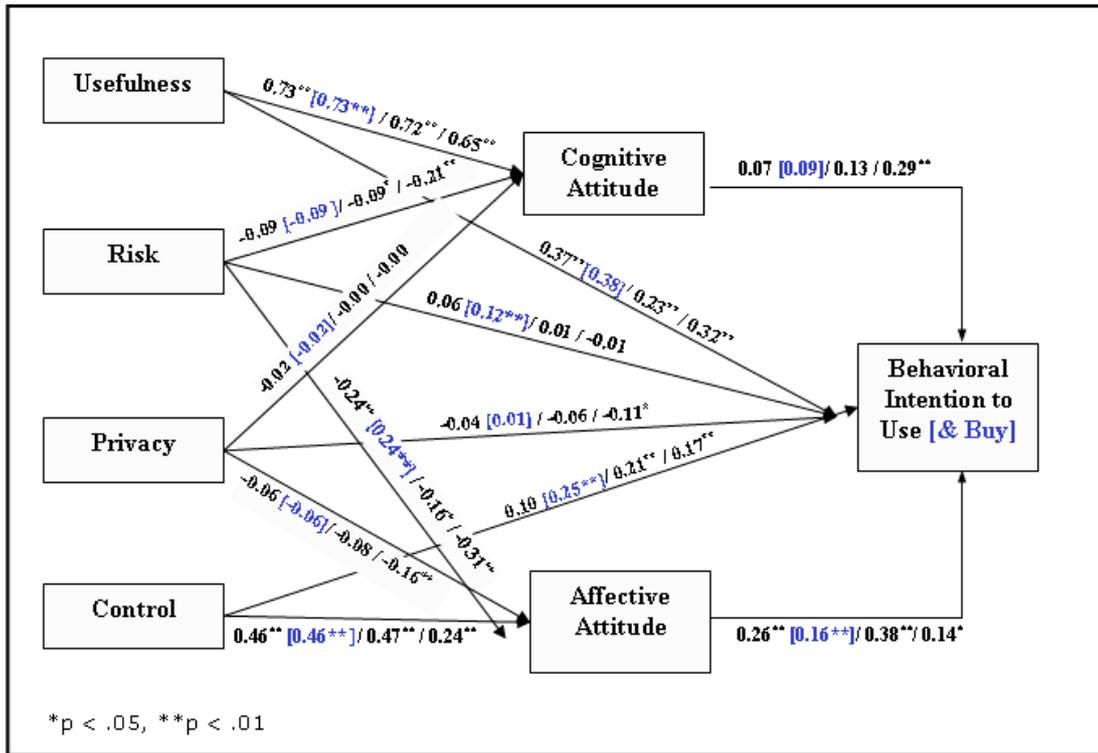


Figure 24: UC-AM: relationships and path coefficients (fridge use [buy] / ISA / garage scenario)

On the overall, R2 results of the UC-AM for use intentions vary from 0.58 for the fridge scenario to 0.68 for the garage service (see table 22). R2 is a measure indicating the predictive power of a model. It is at a satisfying level here seen that R2 measures have on average been between .40 and .45 in the traditional TAM literature [see (Venkatesh, Morris et al. 2003) and our own analysis based on 20 TAM sources].

Table 22: R² results for TAM versus UC-AM

	TAM	UC-AM (Use)	UC-AM (Buy)
Fridge	0.52	0.58	0.70
Intelligent speed adaptation	0.51	0.67	-
Car maintenance / garage	0.56	0.68	-

Finally, we compared the predictive power of the parsimonious TAM model with UC-AM based on the data collected in the present study. Doing so, we found that the parsimonious TAM model with USF and EOU driving BI yields a R2 of 0.52 for the fridge, 0.51 for the speed adaptation and 0.56 for

the garage service. The predictive power of UC-AM is therefore clearly superior to TAM with R2 ranging from 0.58 to 0.68.

Even though these R2 values suggest that TAM has relevance for the comprehension of UC service acceptance a more thorough analysis reveals that TAM would really be reduced to the sole influence USF on BI. This is, because – as expected - ease of use loses its importance in a functioning UC service landscape. Ease of use shows only small to very small correlations with any of the other model constructs. Including it in TAM or in an analogous way into UC-AM thus would not yield any improvement for the predictive power of UC-AM.

4.2.3.3 Testing the UC Acceptance Model for purchase intentions

The hypothetical relationships found for the intention to use any of the three UC services are almost identical to those found for the intention to purchase the smart fridge application. Affective attitude is again the main determinant for the intention to purchase (confirming hypothesis 2). And the cognitive attitude has no significant impact (disconfirming hypothesis 1). Usefulness reflections have almost the same positive and significant influence (confirming hypotheses 3 and 4). And privacy evaluations have no impact on purchase evaluations (disconfirming hypotheses 5, 10 and 11).

For the risk construct, however, we find, interestingly, that when it comes to the decision to purchase the UC fridge service, perceived risk exercises a significant direct influence on the intention to buy (see figure 24). This influence is twice as strong as the one observed for the intention to use. This observation is sensible seen that perceived risk was first recognized in the marketing literature as being particularly relevant to purchase processes (Bauer 1960; Cunningham 1967; Kaplan, J. et al. 1974)

Another noteworthy difference observable for the intention to purchase is the role of perceived control. While control perceptions seem to be largely channelled through affective attitude when it comes to the anticipation of usage, purchase intentions are also directly impacted by control perceptions. Perceived control over the fridge supply service has a significant and strong direct impact on the intention to buy (confirming hypothesis 9). At the same time, the importance of affective attitude is reduced for this scenario. This implies that people can very well imagine using services which deprive them of control, but they are less willing to purchase them.

4.2.4 Discussion: The Value of UC-AM to Explain Service Acceptance

4.2.4.1 How privacy, control and perceived risk influence UC acceptance

The results show that there are some stable constructs relevant for UC service acceptance across scenarios. They equally reveal that some issues raised in the literature may be less relevant for UC service acceptance than expected. Privacy concerns, for example, may be overestimated as a major impediment, at least for the purchase and use of pro-active UC services. Privacy concerns show hardly any influence on BI and on AffATT and an additional correlation analysis reveals that mean factor values are at best moderately related to any other model construct. Equally, they have no impact on the cognitive effort towards a service. This finding goes in line with what privacy researchers have repeatedly observed: peoples' privacy concerns do not drive their behavior (Spiekermann, Grossklags et al. 2001; Acquisti and Grossklags 2005).

Several studies on privacy in e-commerce suggest that privacy concerns and expectations do not determine whether and how people interact with systems. Even if people are made aware of potential

data sharing practices and consider themselves as highly privacy sensitive they do not act in a privacy sensitive way when interacting with systems (Acquisti and Grossklags 2005; Berendt, Guenther et al. 2005). Our data suggests that privacy is simply not at the immediate forefront of peoples' minds when they evaluate a new proactive UC service the essence of which appears to be less about tracking somebody, but instead deliver a service. The only scenario where privacy showed a small, but significant influence is in the garage service. Questions which asked for the concern of secondary use of information on one's car's condition yielded a negative affective response, and slight resistance to use the service while the same practice in the context of information on one's daily nutrition left people uninvolved. This reflection of the scenario background suggests that the role of privacy for UC acceptance may be limited to a few contexts where the type of information at play is particularly sensitive. However, on the overall our data leads us to conclude that privacy may be less important for the acceptance of many UC services than scholars believe. Information collection needed for the purpose of a particular service seems to raise little concern among consumers and if it does the impact on use and purchase intentions is marginal.

Our study also found that perceived control over a service has an important and stable impact for its acceptance. Regardless of the scenario presented to participants', perceived control significantly influenced the affective attitude expressed towards it. And this influence of control over system operations on peoples' emotions is bigger than the influence of any other construct investigated. In two out of three cases it even becomes directly relevant for the intention to use or avoid a service. Moreover, when it comes to the purchase of a system, perceived control more than doubles its direct impact on use intentions. This finding is in line with (Várhelyi 2002) who also reported: "[...] devices to control the speed of cars 'when the driver is free to turn it on or off' were favored by about 46% of the respondents" whereas " [...] a device which 'makes it impossible for all cars to exceed a certain limit' was favored by about 35%" (p. 245), a significantly smaller number. Engineers therefore have to ensure that they are getting the 'control-balance' right when designing proactive UC systems. They should be aware that by allocating functions between users and intelligent objects they are strongly influencing the immediate affective reactions people will show vis-à-vis the system as well as purchase and use intentions.

An open question is whether initial control perceptions will persist. Even though important for the upfront decision to use and buy a service, it cannot be excluded that people also get used to giving up control. Quite a few examples illustrate this. For example, the transition from manual to automatic automobile starters was equally accompanied by a control debate which from today's perspective appears antiquated. Also pilots were shown to prefer automation after they got used to it (Riley 1996). Yet, even if people get used to automation over time the issue remains that too much automation could impinge on the initial propensity to purchase a UC service. A nascent UC market would thus be negatively impacted.

Finally, OPR was shown to exercise an indirect influence on the intention to use a UC service via affective attitude. As outlined above, OPR can furthermore be decomposed into its individual risk dimensions. In particular, (Featherman and Pavlou 2003) suggest that functional risk should be treated as a separate construct from other risk dimensions. Applying this reasoning to the current data set revealed an interesting insight: in fact, functional risk shows no significant influence on attitudes or the intention to use UC services in any of the scenarios. At the same time, the 'personal risk factor' aggregated from psychological, time and financial risk indicators gained in predictive strength and showed consistent significance for both affective and cognitive attitude formation across scenarios. Personal risks associated with a UC service, such as loss of time or lack of fit with one's daily life therefore seem to impact the cognitive evaluation of the service as well as the affective reaction to it.

4.2.4.2 Towards an integrated model for UC service acceptance and the role of distinct attitudes

At the core of UC-AM is the distinction of cognitive and affective attitude. A major question of the empirical work was whether there is a hierarchy of effects with attitude constructs serving as stable

mediators for control, risk, privacy, and usefulness perceptions. And indeed affective attitude seems to serve as a stable mediator for both the perceived risk of a service and the perceived control over it. For the cognitive evaluation, however, we could not observe such an effect. We additionally find that the relative importance of the distinct belief constructs as well as the relative ‘weight’ of the cognitive and affective side for valuing a service differs from one context to another. In the garage scenario, for example, cognitive attitude’s effect (see table 23) is two to four times more important for BI to use than it is in the ISA and fridge scenario. Instead, BI to use the ISA system is largely driven by peoples’ affective reaction towards the service, in particular due to control perceptions. In line with (Trafimow and Sheeran 1998) we therefore observe that the relative importance of affective and cognitive attitudes is strongly moderated by the task. As a result, we would argue that while stable determinative acceptance factors exist for UC acceptance (such as usefulness) and some of them are regularly mediated by affective attitude (such as control and risk) the impact of general attitudes and the relative importance of affect or cognition is varying. Still missing is a taxonomy as to when which construct is as important as the other.

Furthermore, some constructs, such as USF have a strong direct influence on BI. This direct influence is more important than the one mediated via cognitive attitude. As a result, there is no scientific reason to claim a general hierarchy of effects for UC-AM. Attitude constructs are valuable as ‘chunks’ to understand future users’ perceptions of a service. They may therefore signal the appreciation of a service before its deployment. And they allow for structuring the thinking around the acceptance of UC services. But a hierarchy of effects cannot be confirmed for all dimensions influential for UC adoption.

Table 23: Total effects of model constructs on intention to use or buy a UC Service

	Fridge		Intelligent Speed Adaptation	Garage Service
	USE	BUY		
AffATT	0,26	0,16	0,38	0,14
CTRL	0,22	0,32	0,38	0,20
CogATT	0,07	0,09	0,13	0,29
OPR	-0,13	-0,16	-0,06	-0,11
PrivConc	-0,05	0,00	-0,09	-0,12
USF	0,42	0,45	0,32	0,51

Finally, this research focuses largely on attitudes and attitude drivers, and a valuable complement to the present study could have been to test the Theory of Reasoned Action or the Theory of Planned Behaviour (TPB). Other scholars have followed this approach to test private household acceptance of established IS systems (Brown and Venkatesh 2005). Yet, as outlined above the control construct as operationalized by (Ajzen 1985; Ajzen 1991) is conceptually different from feelings of control over service functioning. Furthermore the measurement of ‘subjective norm’ represents a methodological challenge when working with future scenarios. Subjects need to anticipate how those they value may again value a future system. Despite this potential methodological pitfall we did control for the role of subjective norm and trialled its integration into the model with one item. When doing so for use intentions, we found that R2 did hardly improve at all (fridge: 0.59; ISA: 0.67; garage: 0.68). Only in the fridge scenario there is a small and significant path coefficient of .12 leading from subjective norm to BI. This finding is not surprising since the fridge service is the only service in which almost always more than one person is involved. More research would be needed though on deployed services in order to better understand the impact of subjective norm on the BI.

4.2.5 Implications of the UC Acceptance Model for Practice

The results of the study show that engineers need to consider the affective user reactions to systems more than may have been the case in the past. While (Yang and Yoo 2004) find that in a professional work context affective reactions to systems are less relevant for the BI to use, the investigation of UC service acceptance in the current study proves the opposite for systems owned and used by private individuals. Given this continuous effect, engineers need to understand the drivers of such affective reactions. Some of them have been identified in this work. In particular, it seems that engineers need to get the 'control balance' right between humans and machines. This has been a major hypothesis in this work. People want to feel that they have choices left when interacting with systems that have the capability to largely act autonomously. The debate around 'function allocation' between humans and machines which has marked the history of automation (Sheridan 2000) therefore sees its relevancy transferred to the UC service world. The next chapter 4.3 will investigate this particular issue in more detail.

Privacy, in contrast, has turned out to be less relevant for UC service acceptance than some UC scholars seem to anticipate. Does this mean that privacy is not important? The data suggest context dependency of the privacy impact. In the garage scenario privacy did influence BI and AffATT. But how can this context dependency be operationalized for UC engineers? And is there a potential that ignoring the maintenance of privacy in UC system design will simply go unnoticed by consumers? More research is certainly needed in this domain. Equally, a debate may be valuable on whether a respect for peoples' privacy should be embedded in UC systems by default for ethical reasons and regardless of immediate market requirements, which, according to this research are not pressing.

This research also finds that it is not functional risk which is really relevant to users when judging the potential 'cons' of UC system use, but more a reflection of the degree to which the UC system will fit into one's daily life and time schedule. Therefore, marketers of UC services are less dealing with systems that need to address a particular professional function as this has been the case with traditional IS. Instead, they have to think about target segments and their way of going about daily tasks in order to impact the 'risk-equation' relevant for the affective and cognitive evaluation of a UC service. Contextual design techniques (Beyer and Holtzblatt 1998) facilitate the production of such well-fitting products.

Having seen the overall predictive power of UC-AM, the question arises why UC-AM should be adopted in favour of a more parsimonious TAM if the R2 results obtained are only about 10% higher than for TAM at least when it comes to usage intentions. We believe that while parsimony and structure are important for technology acceptance research, concrete insights into the dynamics of those factors needed for prioritizing system design are equally vital. Therefore, we see a major contribution of this research in the proof that the control construct is so vital for affective appreciation of UC systems. After all, affective attitudes and control perceptions can be actively influenced through user interface design (Maes and Wexelblat 1997). Equally, embedding privacy enhancing technologies in UC systems is an option for UC designers. Yet, the findings of this research would suggest that, at least from a commercial perspective, investment in privacy design may be less valued by consumers than is often believed. Certainly, control, risk, privacy and usefulness just mark a starting point for analysing consumer intentions to use UC systems and explain subsequent usage. More research would be valuable that complements the insights into what drives affective and cognitive attitudes towards UC systems. When it comes to the prediction of purchase intentions, UC-AM displays a very high predictive power. A limitation of this research is that we measured purchase intentions for only one out of three scenarios. More research is therefore essential to confirm this finding.

A further limitation of our study is the nature of the sample. We base our analysis mainly on the evaluations of young to middle-aged German adults, which is clearly not representative for a whole population. While this bias admittedly stems from pragmatic reasons, it can be argued on the other hand that especially these people will be in the centre stage of the consumer market when UC services are introduced.

Furthermore we could not investigate possible long-term effects of the introduction of UC services as it is common in the tradition of diffusion of innovation research (Rogers 2003). It was shown that very

often people get used to services which they originally opposed. Pilots and thus people who are highly familiar with automated systems were shown to have a substantial bias in favour of using automated controls (Riley 1996). We argue, however, that the scenario-based approach is less well suited for investigating such questions because it is difficult for people to take dynamic factors into account, such as a technology uptake in one's immediate social environment.

Finally, validating construct relationships across applications is vital for UC research. Many of the first acceptance articles in the context of UC today do not go beyond single-device, single-service testing (e.g. (Várhelyi 2002; Garfield 2005)). They therefore question less the dynamics, which are relevant across a larger group of UC services, such as increased data collection and machine proactivity. Instead, they focus on the particular dynamics of one application only with a limited number of users (Scholtz and Consolvo 2004). The value of the current research is that it identifies generalisable factors of influence which can then again inform the study of individual applications. The trade-off created by such cross-service testing is, however, that it is only feasible on the basis of 'fictive' and controlled service descriptions such as those presented in this study while more concrete studies are able to observe real behavior and real interactions with real systems. We believe that the future lies in the pursuit of both kinds of empirical work.

4.3 About the Importance of Function Allocation for UC Acceptance

The study of UC-AM clearly shows that a perception of control over automation has a direct influence on the affective valuation of a proactive UC service in the private realm. When it comes to purchasing UC services, the influence of control perceptions seems to become even more relevant. Then, not only affective reactions can be observed, but direct implications for a reduced willingness to buy. This stable influence justifies one further investigation of the control construct, namely, into whether a variation of the degree of control by allocating man-machine functions differently would also lead to significant differences in system acceptance. The correlation based relationships observed in UC-AM would suggest that this is the case. But the empirical observation so far only says that those people who had a tendency to feel in control also had a tendency to like the system more and use it more.

However, people are sometimes apt to illusions of control (Langer 1975). They often feel more in control than they actually are. Also, depending on personality (Rotter 1954) and demographic factors (Thompson and Spacapan 1991) some people generally feel more in control than others and this is regardless of the underlying system. Perhaps it could even be that those people who think more bullish about their own levels of control have a systematic tendency to also show more positive affective attitudes towards the things around them. These arguments elicit the need to confirm that people who factually have more or less control over systems would also intent to use them more or less often. Does the observed relationship between control and affective attitude as well as between control and use or purchase intentions hold true if people are confronted with two different system control designs?

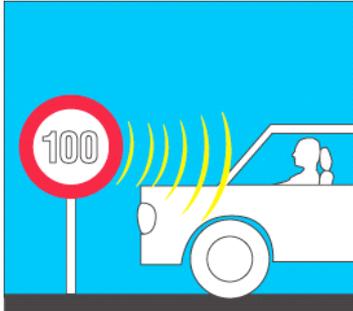
In order to investigate this question we draw upon another empirical study which we conducted with the same set-up a year earlier. Even though the study was conducted a year earlier we will call it hereafter 'study 2' in order to respect the sequence of its presentation in this work. Study 2 was marked by the fact that the same UC systems tested for UC-AM were investigated again, but deliberately varied with respect to the degree of user control. As will be described below, the variation was such that one version of the same system (for example, the fridge) was described to study participants as automizing the entire UC service experience. Thus, machines would act completely autonomously. The wording used here was identical with the one described above for UC-AM. An alternative scenario version then described the same system in a different fashion: here, less system automation was implied in the sense that users would need to confirm machine activities. The crucial difference between the two scenario versions is the degree of automation inherent in the system: in one variation the 'last word' remains with the user. In the other it is with the machine. The degree to

which decision making and activity is shared between humans and systems has been termed ‘function allocation’ and in section 2.3.4.2 above we already gave a short introduction to this problem domain in classical automation engineering. Figure 25 shows the subtle manipulation used to present two alternative system designs. Our hypothesis was that leaving the last word with the user would lead to a higher service acceptance and thus more positive affective evaluation as well as increased use and purchase intentions.

Intelligent Speed Adaptation (ISA)

“It is the year 2015...

My car has become intelligent by the help of numerous sensors. The intelligent functions above all are meant to increase my driving security. One of these intelligent functions is the automatic speed limit. This function is an obligatory legal regulation to all cars, except for police, ambulance and fire brigade. The system works such that speed limit signs send radio signals to my car, transmitting the required speed limit to it”

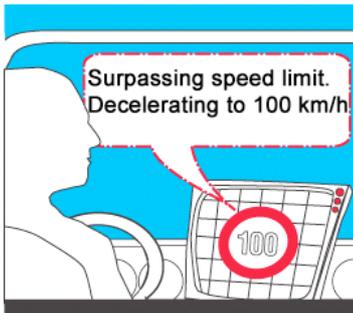


The Intelligent Speed Adaptation System

What the system looks like

For group 1 (low control) the text continued...

“If I am driving too fast, my car automatically decelerates. The navigation system informs me that it has automatically decelerated in order to stay within the speed limit.”

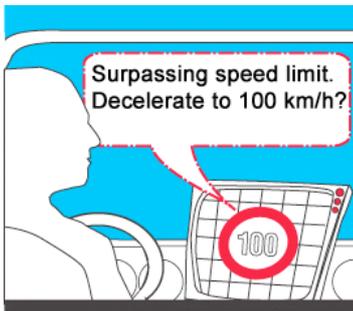


What the controls look like:

Low control

For group 2 (high control) the text continued...

“If I am driving too fast, my car automatically notices this violation. The navigation system recommends me to brake in order to stay within the speed limit.”



What the controls look like:

High control

Figure 25: Two different potential man-machine function allocations for ISA

4.3.1 Methodology: A Scenario Based Variation of Function Allocation

4.3.1.1 The development of the stimulus and instruments used

In section 4.2.2.1 above we described how UC scenarios were selected in study 1 and tested (see also appendix 5 for an overview). The same scenarios were used in study 2 except for one additional scenario relating to an adaptive desktop system. The desktop scenario read as follows: “It is the year 2015...my intelligent desktop at home is equipped with a PC, a phone and a small camera (webcam). All devices hook up automatically to form a network. Many intelligent functions are integrated in the desktop environment which aims to facilitate my work. One function of the intelligent desktop is that it always recognizes automatically what I am doing and supports me in my activities....”

At the end of each scenario description one sentence was varied with a view to the degree of automation. Figure 26 gives an example on how this variation was formulated and depicted for the desktop scenario.

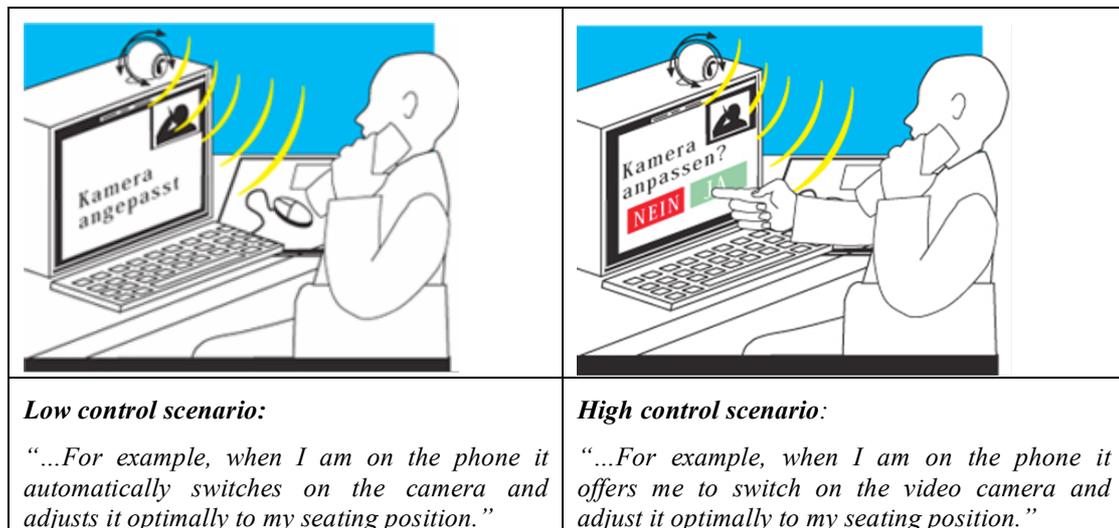


Figure 26: Control groups variation: Example of the adaptive desktop system

The descriptions of user control were derived from Sheridan’s hierarchy of automation control as they have been described in chapter 2.3.4.2 (Sheridan 1988; Sheridan 2002). For every scenario we contrasted levels 4 and 6 of the control hierarchy. Level 4 reads “The computer selects one way to do a task and executes that suggestion if the human approves” whereas level 6 says “The computer selects on way to do the task and executes automatically, then necessarily informs the human” (p. 62 in (Sheridan 2002) and table 3). Level 6 is regarded as providing the user with lower control over the system and thus is called the “low control” group hereafter, whereas level 4 is referred to as the “high control” group.

Question items to measure affective attitude and use intentions, as well as evaluations of usefulness, were the same in study 2 than they were for the UC-AM study (see appendix 8).

4.3.1.2 Setting and data collection procedure

The study was conducted as an online survey posted on the Internet for four weeks in November 2005. The online survey was advertised by a large German newspaper called DIE ZEIT and subsequently promoted by other media channels such as one of Germany's main IT news platforms (heise.de). Participants were informed that the results would be part of a government-funded technology assessment study on Ubiquitous Computing. Perhaps as a consequence of this strong media advertisement 4.744 participated in the study. As we gave participants the choice to comment on either two, three or four scenarios only 3675 people (77%) evaluated all four scenarios. They invested an average time of 37 minutes in this process. 1776 of them saw the low-control-version of the technologies, 1899 the high-control-version. As can be seen from table 24 the demographic distribution of the online sample shows a strong self-selection bias. Mostly well educated men participated here. Self-selective bias is a problem often encountered in online surveys (Baltinic, Reips et al. 2002). For this reason, the study was conducted in parallel on paper and pencil via a marketing agency. Here, 200 persons were contacted randomly in four distinct German regions and then selected to approximately mirror German demographics. As a result, demographics are much more balanced. Table 24 compares the demographics of the two samples.

Table 24: Demographics of two samples of participants of the 2nd UC Acceptance Study

		Market Agency Sample	Online Sample
		200	3675
sex	male	49%	81%
	female	51%	19%
age	< 30	24%	46%
	30-39	20%	26%
	40-49	29%	16%
	>49	27%	12%
education	no A-levels	57%	10%
	A-levels	18%	36%
	university degree	25%	54%

For both samples participants were randomly assigned to one of the two control conditions and were then presented all four scenarios either in the low-control version or in the high-control version. We chose a between-subject experimental design for the reasons outlined above, aiming to exclude a systematic and uncontrolled error that could be due to a participants' control-related personality traits. Equally, within-subject designs often bear the risk of carry-over-effects (Poulton 1973) which for our case would have meant that participants answer in the same way to both distinct scenarios due to not realizing that they are different. On the other hand, a within-subject design could have been preferable on statistical grounds as well (Greenwald 1976; Keren 1993) seen that the same person – assuming that she recognizes the difference – also corresponds differently to the respective control version.

The order of the scenarios was randomized in order to control for possible sequence effects.

4.3.2 Results: Perceptions and Effects of Function Allocation

The first analysis relevant in this context was whether indeed the distinct levels of control are perceived by study participants as providing them with significantly different degrees of control. Only if this hypothesis is confirmed we can attribute further differences between groups to the different levels of perceived control over the system. Methodologically, t-tests for independent samples were

carried out to test for significant differences between the experimental groups. These test results, their significance levels, means and standard deviations of all constructs are given for the total sample and each experimental control group in table 25. Since the significance testing using t-tests is sensitive to sample size, the effect size was equally calculated in form of the Pearson correlation coefficient r , which was computed as proposed by (Rosenthal 1991). Values of r above .1 can be considered as small effects, beyond .3 as medium effects and beyond .5 as big effects (Cohen 1988).

Table 25: Differences in constructs between low- and high control groups (online sample)

Construct	Scenario	Experimental Groups						T-Test			
		Total Sample (N=3675)		Low Control (N=1776)		High Control (N = 1899)		t	df	Sig.	r
		M	SD	M	SD	M	SD				
Perceived Usefulness (USF)	Intelligent Fridge	3,31	1,21	3,25	1,24	3,37	1,19	-2,95	3635	0,00	0,05
	Intelligent Workplace	3,13	1,23	3,12	1,23	3,15	1,23	-0,70	3672	0,49	0,01
	Intelligent Speed Adaptation	2,72	1,09	2,70	1,11	2,74	1,07	-1,27	3673	0,21	0,02
	Automatic Car Maintenance	3,60	1,09	3,53	1,11	3,68	1,06	-4,13	3628	0,00	0,07
Perceived Ease of Use (EOU)	Intelligent Fridge	4,05	0,96	4,02	0,97	4,08	0,94	-1,81	3673	0,07	0,03
	Intelligent Workplace	3,52	1,17	3,54	1,15	3,50	1,20	0,90	3669	0,37	0,01
	Intelligent Speed Adaptation	4,39	0,80	4,41	0,80	4,37	0,80	1,43	3673	0,15	0,02
	Automatic Car Maintenance	3,99	1,02	3,96	1,04	4,03	1,00	-2,03	3632	0,04	0,03
Intention to Use (BI)	Intelligent Fridge	3,33	1,25	3,27	1,28	3,39	1,21	-3,07	3673	0,00	0,05
	Intelligent Workplace	3,31	0,97	3,28	0,97	3,34	0,98	-1,81	3673	0,07	0,03
	Intelligent Speed Adaptation	3,20	1,22	3,12	1,23	3,28	1,21	-3,82	3673	0,00	0,06
	Automatic Car Maintenance	3,46	0,98	3,37	1,00	3,54	0,95	-5,21	3673	0,00	0,09
Intention to Buy (BI)	Intelligent Fridge	2,83	1,39	2,75	1,40	2,91	1,38	-3,56	3673	0,00	0,06
	Intelligent Workplace	2,63	1,33	2,58	1,33	2,67	1,33	-2,08	3672	0,04	0,03
Affective Attitude (ATT) ^{a)}	Intelligent Fridge	3,14	1,05	3,08	1,07	3,20	1,02	-3,57	3673	0,00	0,06
	Intelligent Workplace	2,81	1,06	2,75	1,07	2,87	1,04	-3,42	3672	0,00	0,06
	Intelligent Speed Adaptation	2,92	1,15	2,85	1,20	3,00	1,09	-3,97	3673	0,00	0,07
	Automatic Car Maintenance	3,36	1,00	3,26	1,04	3,46	0,95	-6,00	3673	0,00	0,10
Perceived Control (CTR)	Intelligent Fridge	2,99	1,26	2,88	1,26	3,09	1,26	-5,07	3673	0,00	0,08
	Intelligent Workplace	2,83	1,24	2,76	1,26	2,88	1,21	-2,89	3672	0,00	0,05
	Intelligent Speed Adaptation	2,60	1,23	2,25	1,14	2,92	1,21	-17,18	3673	0,00	0,27
	Automatic Car Maintenance	2,84	1,24	2,61	1,22	3,06	1,23	-11,33	3673	0,00	0,18

Note: ^{a)} Higher values reflect more positive attitudes

The results of the larger online sample show that participants indeed perceived a significantly different level of control depending on the scenario version they saw and this was true for all scenarios. In absolute terms the data show that the intelligent speed adaptation system is perceived as the biggest violation of user control. Here, the effect size (r) approaches a medium level.

Furthermore, participants in the low-control group evaluated all technologies significantly worse in terms of affective attitude than did their counterparts in the high-control group. In other words, they felt more sadly envisioning interaction with low-control-systems and were less willing to use these systems. The effect sizes of these differences are, however, very small. The differences in affective attitude are most prominent in the car maintenance system. Perhaps as a consequence the intention to use this kind of system is then also lowest for the car maintenance system in the low control condition. Interesting enough, the intention to use an adaptive desktop system is the least affected by the control manipulation. Even though the control manipulation was perceived and affective reactions showed significant differences, people do not show the same dynamics when it comes to their use intentions. This finding supports earlier studies on technology acceptance where intentions to use professional desktop systems seemed less related to affect (Davis, Bagozzi et al. 1989).

When comparing the young, male and tech-affine group who participated in the online study with the one who filled out the paper and pencil questionnaire a striking difference becomes apparent: Paper participants felt significantly more in control over all technologies described to them than the online sample in both control variations. Thus, when an 'average' citizen in terms of age, education, income, etc. is confronted with the low control scenarios he or she feels less out of control than when young, tech-affine and well educated people reflect on the scenarios. Table 26 summarizes this finding as well as all other judgements found for the paper sample. Also the difference between the control manipulations is less felt by the paper sample than by the online sample. The difference in perceived control due to the manipulation of function allocation does not reach statistical significance in the fridge and workplace scenario. Where it does reach statistical significance – in the car scenarios – people who perceive less control are again less positive about the service in terms of emotion and are less likely to use them. Unlike the online sample, however, purchase intentions are not significantly different for the two control groups.

Given these differences between the two demographically distinct groups, the question arises as to whether these can be explained with any of the demographic data we collected; in particular gender, age or education. As far as gender is concerned, an interesting separating line seems to exist between the home applications (desktop and fridge) and the car scenarios (ISA and garage): When control is low, men seem to be less impacted than women. They continue to have a higher affective attitude towards home automation, they feel more in control than females and are more likely to purchase and use them. The tendency in the data suggests that women may be less enthusiastic of being deprived of what some could consider their duty. In the speed adaptation scenario, in contrast, this is precisely the opposite. Here men feel less empowered, like it less, and find it less useful even though the reduced willingness to use it is not statistically significant. These slight absolute trends in the data do not reach statistical significance in the smaller paper sample but are mostly significant (at $p < .05$) in the online sample (see tables 2 and 3 in appendix 9). It therefore cannot be argued based on the current data set that women and men exhibit distinct control desires and perceptions in line with their traditional roles in the house or outside. But a slight tendency can be observed in the patterns of the data collected. Other sources have also reported that men and women hold different control beliefs (Thompson and Spacapan 1991)

When it comes to age differences another interesting trend is uncovered by the data: Regardless of the control manipulation, older people (beyond 50 years of age) generally tend to perceive more control than younger people (below 30 years of age). The only exception from this trend can be observed for the adaptive desktop scenario. But here it could be argued that prior negative experience of the elderly with computers may have led to the results. Again, the data pattern must be regarded with caution. Except for one case, the trend does not reach statistical significance in the paper sample, but it does so in the online sample. For the car scenarios, r values above .10 support the existence of a small effect. Again, findings by other researchers support this observed tendency. It was found that older workers have fewer control concerns than younger colleagues and that from adulthood onward there is a norm for increased specificity with respect to the domain in which one exercises control (reported in (Thompson and Spacapan 1991).

For the level of education no consistent data pattern hints to a relationship of this characteristic with the perception of distinct function allocations.

Table 26: Differences in constructs between low- and high control groups (paper sample)

Construct	Scenario	Experimental Groups								T-Test	
		Total Sample (N=200)		Low Control (N=96)		High Control (N = 104)		t	df	Sig.	r
		M	SD	M	SD	M	SD				
Perceived Usefulness (USF)	Intelligent Fridge	3,58	1,26	3,50	1,36	3,66	1,15	-0,94	198	0,35	0,07
	Intelligent Workplace	3,37	1,26	3,35	1,35	3,39	1,19	-0,19	198	0,85	0,01
	Intelligent Speed Adaptation	2,93	1,11	2,73	1,09	3,10	1,11	-2,38	198	0,02	0,17
	Automatic Car Maintenance	3,89	1,03	3,64	1,14	4,11	0,87	-3,30	198	0,00	0,23
Perceived Ease of Use (EOU)	Intelligent Fridge	3,98	1,02	4,01	1,04	3,96	1,02	0,31	198	0,76	0,02
	Intelligent Workplace	3,46	1,18	3,40	1,23	3,51	1,13	-0,64	198	0,52	0,05
	Intelligent Speed Adaptation	4,27	0,89	4,15	0,98	4,38	0,79	-1,83	198	0,07	0,13
	Automatic Car Maintenance	3,95	1,02	3,86	1,09	4,03	0,95	-1,14	198	0,26	0,08
Intention to Use (BI)	Intelligent Fridge	3,27	1,37	3,32	1,44	3,23	1,30	0,46	198	0,65	0,03
	Intelligent Workplace	3,42	1,00	3,44	1,05	3,41	0,96	0,22	198	0,83	0,02
	Intelligent Speed Adaptation	3,56	1,21	3,43	1,31	3,68	1,09	-1,50	198	0,14	0,11
	Automatic Car Maintenance	3,77	0,92	3,61	1,02	3,92	0,79	-2,40	198	0,02	0,17
Intention to Buy (BI)	Intelligent Fridge	3,05	1,44	3,05	1,58	3,05	1,32	0,00	198	1,00	0,00
	Intelligent Workplace	2,71	1,37	2,72	1,43	2,71	1,32	0,06	198	0,95	0,00
Affective Attitude (ATT)^{a)}	Intelligent Fridge	3,08	1,08	3,12	1,13	3,04	1,04	0,53	197	0,60	0,04
	Intelligent Workplace	2,86	1,10	2,82	1,10	2,90	1,11	-0,49	198	0,63	0,03
	Intelligent Speed Adaptation	3,21	1,12	3,06	1,13	3,34	1,10	-1,78	197	0,08	0,13
	Automatic Car Maintenance	3,68	0,96	3,48	1,07	3,86	0,80	-2,85	197	0,01	0,20
Perceived Control (CTR)	Intelligent Fridge	3,26	1,27	3,25	1,39	3,26	1,16	-0,10	195	0,92	0,01
	Intelligent Workplace	3,22	1,40	3,15	1,38	3,29	1,42	-0,72	198	0,47	0,05
	Intelligent Speed Adaptation	3,04	1,25	2,58	1,19	3,45	1,17	-5,16	197	0,00	0,34
	Automatic Car Maintenance	3,31	1,44	3,04	1,46	3,55	1,38	-2,54	197	0,01	0,18

Note: ^{a)} Higher values reflect more positive attitudes

Summing up, the data suggests that the control manipulation is indeed felt by individuals even if it is very subtle. In line with our hypothesis and the findings in chapter 4.2 above, less control leads to a reduction in affective attitudes as well as less propensity to buy and use a service. However, contextual variables such as the nature of a service as well as the demographic characteristics of a consumer (such as age and gender) could play a role in service perception that leads to more or less reactions to control variations. Even if this finding is statistically not sound enough to be generalisable upon the current data set, it could still be used as an indication for the existence of these differences. This again speaks for cautious consideration of demographics in the design of UC systems and the determination of automation levels in line with potential target customer segments.

5

Conclusion

Typically Ubiquitous Computing research conducted by engineers is driven by the desire to enhance and solidify technological capabilities. It is characterized by investigating what technology could do and how it should optimally function when hardware, software, networking, energy and other natural and technical constraints are present. This work, however, is different. It tries to look at UC from an end-user perspective and asks what goals the evolving technological landscape pursues with the diverse applications it creates. These value propositions are being opposed with the still existing pitfalls and challenges accompanying the introduction of UC technologies.

We offer a new way of looking at Ubiquitous Computing: to equate it with automation and to plainly view UC as the automation of everyday life. Many UC scholars will object to this demystifying idea. But in chapter 2 of this work we give proof of the many parallels between UC and automation.

Literature on and experience with automation has been accumulated since its rise in the 19th century and hence UC, being a relatively young research stream may have a lot to learn from the classic discipline.

This work contributes something new and important: It systematically transfers the classes and goals, many challenges and models of automation to Ubiquitous Computing. By doing so, it contributes to the theory building of the young discipline, defining some frames of reference and models needed to structure technical visions and fantasies.

Intuitively, when we talk about automation we feel that the term is associated with the idea to replace manual tasks and relieve us of repetitive or heavy physical burdens. Equally, technicians immediately think of closed-loop control systems. But when looking into the newer automation literature it becomes apparent that increasingly the discipline is also about the reliable collection and combination of myriad data sources (in particular sensor data), the handling and interpretation of rich data volumes that cannot be achieved by the human mind alone and the use of this information base for better decision making.

Scholars in automation research have started to talk about ‘information automation’ and input automation and they distinguish this area of activity from the traditional output automation. When analysing the goals of 30 current UC applications in chapter 2 it becomes apparent that in fact 93% of them are falling into the category of input automation. UC technicians report on video systems and sensor networks, RFID reader landscapes and infrared systems, all of which are essentially about the ability to collect information in an automated way. The technologies allow us to see things which were not accessible to us in the past: our own performances, states, whereabouts, social network activities, compatibilities to name a few.

That UC works on input automation may be surprising for those who claim that Ubiquitous Computing is primarily about pro-active and calm computing and aims for factual service delivery. However, not even 10% of the application snapshot we analysed are living up to this pro-active service vision. Consequently, a provocative question could be: Where is this calm (service delivery) in calm computing?

In fact, calmness seems to set in when it comes to the calm and automated collection of information: 86% of the applications analysed in chapter 2 enable us to simply see and perceive more than we ever did before. We are finally enhancing our senses, creating something which could also be called ‘ubiquitous presence’.

For sure, humans have always been interested in seeing more than they were able to physically. Christian theology reserves the talent of ubiquitous seeing to ‘God’. French language embeds the word ‘seeing’ (=“voir”) into its term for knowledge (=“savoir”) and power (=“pouvoir”). This perspective on UC is indeed something that has rarely been discussed by scholars; potentially not even explicitly recognized.

Through its highly structured and in-depth analysis of 30 UC applications this work helps to clarify what UC applications to date are really all about and where there is potential for them to evolve.

We address the ability to see more or the information collection part of UC here in the context of one particular technology, RFID. We identify the main areas of consumer concerns and lead a critical discussion of how these concerns can be technologically addressed. Because a recent EU-wide study among over 2000 citizens revealed that 70% believe that privacy protection measures for RFID will mostly emerge from technological solutions (Commission of the European Communities 2007), the relevance of this subject domain becomes apparent.

Quite a few market studies on RFID have observed that consumers are concerned about the potential automatic data collection introduced through RFID item-level tagging. Policy debates on privacy are being conducted as part of the decision-making process on the technology’s roadmap. An active community of UC researches has dedicated itself to develop privacy enhancing technologies for RFID. The research presented in chapter 3 is directly contributing to these efforts.

We present a qualitative analysis of consumer concerns which is the first to our current knowledge that tries to isolate concrete user concerns and their underlying reasons.

Our findings lead us to not share in the claim that people are generally concerned to be read out automatically by RFID readers (in fact, they often like to be read out if this is beneficial for them; e.g. to enable seamless access controls). Instead, people seem to be concerned that their personal belongings could be assessed, without knowledge and control and in unexpected contexts. Thus, we identify the psychology of ownership, humans’ inherent territorial thinking and the desire for control as crucial parameters for the acceptance of RFID read processes. Furthermore, consumers do not appreciate being classified upon the data collected, ubiquitously followed by the eyes of the infrastructure in shared territory and restricted in the use of one’s proper belongings.

Against the background of consumer concerns and long existing insights into the psychology of control, we deduct three main control requirements for consumers in RFID enabled environments which clarify what RFID PET engineers should be striving for.

First, RFID PETs should be designed to provide their users with cognitive control over when RFID read-outs occur. Second, decisional control is needed to determine when RFID based data collection should be allowed to happen. And third, behavioural control in the sense of stopping tag-reader communication is required. This fan of control desires should be the benchmark for RFID PET engineers.

Interesting enough, though, our analysis of current privacy enhancing technology proposals for RFID reveals that over 80% of scientific contributions exclusively focus on the security of the air interface between tags and readers. In these works none of the three control requirements is fulfilled. We therefore lead a critical discussion of current privacy enhancing technologies for RFID and reflect on the few existing proposals to give people control over RFID information flows between tags and readers.

Based on a snapshot analysis of 71 papers published on end-user privacy in RFID environments, we identify two main technological approaches as useful to control

information flows between RFID tags and readers: the Agent Scheme and the User Scheme.

In the Agent Scheme, people would have personal agents supervising information flows for them. They would thus delegate privacy management to a privacy device. However, looking into the details of current Agent Schemes three key technical advancements are still necessary for their proper functioning: One is that one-to-one tag-reader communication needs to be preventable for probabilistic protocols by a mediating privacy device. The second is the standardized recognition of privacy preferences in tag-reader communication protocols. And the third is the advancement of reliable privacy context modelling and context recognition. If these three scientific challenges are not satisfactorily solved, Agent Schemes bear little potential to become truly useful and cost efficient in the future.

Besides the precise uncovering of the open research needs for the realization of Agent Schemes, we also propose our own RFID protection solution: The User Scheme.

The User Scheme can be implemented in a much easier way, because no complex technological changes to tag-reader protocols would be required. Also the solution would be less costly and offer the highest degree of objective as well as perceived control to people, because people do not need to trust an agent device, but their own judgements. Tag- reader communication would be blocked by default and people would themselves initiate information exchange where needed.

By this we argue that the development of RFID infrastructures would take a different route if the User Scheme was the privacy solution of choice. As people self-initiate read-outs in the User Scheme the number of read points would probably evolve to be less ubiquitous and concentrated in those areas where they provide the most benefit to people. In the Agent Scheme, in contrast, the RFID infrastructure is in a pro-active initiator role and thus more economic incentive exists to set up a seamless reader infrastructure. We therefore make the case for engaging more in privacy engineering and process modelling with a User Scheme in mind.

That said, we must however acknowledge that our quantitative analysis of RFID PET acceptance suggests a general disapproval of any complex PET solution.

This work is the first of its kind to empirically investigate RFID PET perception, including proper scale development and statistical testing of technological options with a critical mass of users.

Our empirical study series with 540 participants (presented in section 3.6) shows that people have no significant preference for either User or Agent Scheme. In contrast, both PET schemes lead people to rather feel helpless vis-à-vis RFID reader infrastructures and they clearly and plainly opt in favour of killing RFID tags at shop exits. No personal attributes, attitudes towards new technologies in general, trust in retailers or privacy consciousness explains this final preference. Mainly, people do not want to use the User Scheme because they finally don't trust its protective abilities. They do not feel that they can control the information collection process triggered by RFID readers. We conclude that more research in trust building mechanism and trust signalling for PETs seems to be dearly needed.

For retailers and other marketers who want to deploy RFID on individual items, the findings must be alarming. If the majority of ordinary consumers (over 60%) wants to kill RFID chips at store exits and appreciated after-sales benefits are rather forgone than accepting functioning chips, retailers need to ask the question how to best tackle this customer issue. Not surprisingly, leading business scholars have raised the debate in such reknown journals as Harvard Business Review (Fusaro 2004).

Beyond the in-depth analysis of automated information collection (input automation) through RFID, this present work has also presented a thorough reflection on the vision of UC scholars to create pro-active and autonomous service environments. Even though the application analysis in chapter 2 suggests that these services seem to be less elaborated and diffused yet, they still represent a major promise of the new computing landscape. As a result, UC engineers will need to be aware of the major dimensions influencing the acceptance of their service creations.

This work contributes significantly in identifying a number of factors which display a significant impact on the intention to use and buy pro-active UC systems.

In particular we prove the high relevancy of affective attitude for use and purchase intentions and its dependency on service risk and control perceptions. Across four UC scenarios, we propose and test the validity of a new acceptance model for UC which we call 'UC Acceptance Model' (UC-AM).

The determinative power of positive emotions is, hence, clearly documented for UC service acceptance. We highlight the importance of control perceptions for these positive emotions. The more control a person perceives over a UC service described to her the more she enjoyed it and could imagine to use it. More important even for marketers, our data suggests that more control, and the last word in a largely automated decision making process, increases peoples' willingness to purchase UC services. These results should sensitize engineers that no gain can be made from fulfilling the vision of calmness if people are not willing to purchase and use such systems. At the same time cognitive evaluations seem to play a much smaller role for UC acceptance than this is the case for IS adoption in professional environments.

Interestingly our study finds that privacy concerns seem to play a much smaller role than expected by some when it comes to peoples' evaluation of pro-active UC services.

Even though these UC services could equally collect myriad personal data from consumers, people do not have privacy at the forefront of their mind when they are confronted with them. Consequently, we cannot conclude from our present data that privacy concerns will play a major role for UC service take-up. A normative question could, however, be raised on whether privacy should be legally provisioned even if people do not seem to base purchase and use intentions upon them.

Finally, the UC Acceptance Model we proposed and tested here contributes to a very early stage of theory building on Ubiquitous Computing. Ideally, we will successively succeed in better understanding the dynamics that underlie cognitive and affective attitude construction in UC environments. We believe that a particular value of our analysis resides in the fact that we could prove model relationships to be viable across distinct service scenarios. Also the very large sample of around 4000 participants in two subsequent studies adds credibility to the results.

We believe that the UC Acceptance Model we propose is well suited to serve as a baseline model for acceptance research on UC similar to the Technology Acceptance Model (TAM) used to investigate the acceptance of professional desktop applications.

Many more antecedents of affect and cognition could certainly be investigated for UC based on our model. For example, it would be interesting to understand the impact of beauty and other hedonic qualities on service acceptance. More insights are certainly needed on when affect dominates cognition and vice-versa. And, is there a rule according to which we attribute one or another factor more or less to the distinct attitude chunks?

No matter what empirical research we conduct with future users, though, this work is and those to come are limited because they heavily reside on assumptions about the future - assumptions we make about the type of technology, the architectures, and the kind of services which will most likely be deployed at some point to come. If we want to conduct research, however, that is 'prospective' in nature then we also cannot circumvent scenarios and need to improve our methodologies to construct and test them in a scientifically sound way.

Methodologically this work is one of those pioneering the approach of applying sound empirical analysis and testing to vaguely probable scenarios.

Perhaps we will never have intelligent fridges in our homes or drive self-servicing cars. This we cannot exclude. But the dynamics of affect and cognition, and the importance of exercising control over UC environments will remain to be important for market success and they will impact our purchase and use behavior regardless of what we conceive our future service worlds to look like.

6

References

- Abowd, G. D. and E. D. Mynatt (2000). "Charting Past, Present, and Future Research in Ubiquitous Computing." *ACM Transactions on Computer-Human Interaction* 7(1): 29-58.
- Abramson, L. Y., M. E. P. Seligman, et al. (1978). "Learned helplessness in humans." *Journal of Abnormal Psychology* 87(1): 49-74.
- Ackerman, M. S., L. F. Cranor, et al. (1999). "Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences". 1st ACM Conference on Electronic Commerce, Denver, Colorado, US.
- Acquisti, A. (2004). "Privacy and Security of Personal Information". in: *The Economics of Information Security*. Eds.: J. Camp and R. Lewis. Boston Dordrecht London, Kluwer.
- Acquisti, A., A. Friedman, et al. (2006). "Is there a cost to privacy breaches? An event study analysis". 3rd International Conference on Intelligent Systems (ICIS), Prague, Czech Republic
- Acquisti, A. and J. Grossklags (2005). "Privacy and Rationality in Individual Decision Making". *IEEE Security & Privacy*. 3(1): 26-33.
- Adams, A. (2000). "Multimedia information changes the whole privacy ballgame". 10th International Conference on Computers, Freedom and Privacy (CFP 2000), San Francisco, USA.
- Adams, A. and A. Sasse (1999). "Taming the Wolf in Sheep's Clothing: Privacy in Multimedia Communications". 7th Conference on Multimedia, Orlando, Florida, USA.
- Adams, A. and A. Sasse (1999). "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.
- Ajzen, I. (1985). "From intentions to actions: A theory of planned behavior". in: *Action-control: From cognition to behavior*. Eds.: J. Kuhl and J. Beckmann. Heidelberg, USA, Springer: 11-39.
- Ajzen, I. (1991). "The Theory of Planned Behavior." *Organizational Behavior and Human Decision Processes* 50: 179-211.
- Ajzen, I. (2002). "Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior." *Journal of Applied Social Psychology* 32(4): 1-20.
- Ajzen, I. and M. Fishbein (2005). *The Influence of Attitudes on Behavior*. Mahwah, New Jersey, USA, NJ: Erlbaum.
- Alben, L. (1996). "Quality of experience: defining the criteria for effective interaction design." *Interactions* 3(3): 11 - 15
- Albrecht, C. (2006). *SPYCHIPS: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move*. Nashville, Tennessee, USA, Plume (Penguin).
- Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Monterey, California, USA, Brooks/Cole.
- Annacker, D., S. Spiekermann, et al. (2001). "E-privacy: A new search cost dimension in online environments". 14th Bled Conference of Electronic Commerce, Bled, Slovakia.

- Ariely, D. (2000). "Controlling the Information Flow: Effects on Consumers' Decision Making and Preferences." *Journal of Consumer Research* 27(2): 233-248.
- Averill, J. R. (1973). "Personal control over aversive stimuli and its relationship to stress." *Psychological Bulletin* 80: 286-303.
- Avoine, G. (2007). "Security and Privacy in RFID Systems." *Electronic Source*. Retrieved June 6th, 2007, from <http://lasecwww.epfl.ch/~gavoine/rfid/>.
- Bagozzi, R., M. Gopinath, et al. (1999). "The Role of Emotions in Marketing." *Academy of Marketing Science* 27(2): 184-206.
- Baier, G. (2004). "Kontrollüberzeugungen im Umgang mit Technik: Ein Persönlichkeitsmerkmal mit Relevanz für die Gestaltung technischer Systeme". Institute of Psychology. Berlin, Humboldt University. Ph.D.
- Baier, G., M. Rothensee, et al. (2006). "Die Akzeptanz zukünftiger Ubiquitous Computing Anwendungen". *Mensch und Computer 2006*, Gelsenkirchen, Germany.
- Baltinic, B., U. Reips, et al. (2002). *Online Social Sciences*. Seattle, WA, Hogrefe & Huber.
- Bandura, A. (1977). "Self-efficacy: Toward a unified theory of behavioral change." *Psychological Review* 84: 191-215.
- Bandura, A. (1989). "Human agency in social cognitive theory." *American Psychologist* 44(9): 1175-1184.
- Batina, L., J. Guajardo, et al. (2006, July 4th, 2006). "An Elliptic Curve Processor Suitable For RFID-Tags." *Cryptology ePrint Archive Electronic Source*, from <http://eprint.iacr.org/2006/>.
- Bauer, R. (1960). "Consumer behavior as risk taking". 43rd Conference of the American Marketing Association, Chicago, USA.
- Bellotti, V. and A. Sellen (1993). "Design for Privacy in Ubiquitous Computing Environments". 3rd European Conference on Computer Supported Cooperative Work (ECSCW'93), Milan, Italy.
- Berendt, B., O. Guenther, et al. (2005). "Privacy in E-Commerce: Stated Preferences vs. Actual Behavior." *Communications of the ACM* 48(4): 101-106.
- Berthold, O. (2005). "Datenschutzgerechte RFID-Technologie". *GI Jahrestagung Sicherheit 2005*, Regensburg.
- Berthold, O., H. Federrath, et al. (2001). "Web MIXes: A system for anonymous and unobservable Internet access". *Workshop on Design Issues in Anonymity and Unobservability*, Heidelberg, Germany.
- Berthold, O., O. Guenther, et al. (2005). "RFID Verbraucherängste und Verbraucherschutz." *Wirtschaftsinformatik* 47(6): 422-430.
- Berthold, O., S. Spiekermann, et al. (2005). "'Data Protective Radio-Frequency Identification (RFID) System by Means of an Owner Controlled RFID-Tag Functionality'". E. P. Office. Europe. PCT/DE2005/000648.
- Bettman, J. R., E. Johnson, et al. (1990). "A componential analysis of cognitive effort in choice." *Organisational Behavior And Human Decision Processes* 45(1): 111-139.
- Beyer, H. and K. Holtzblatt (1998). *Contextual Design - Defining Customer-Centred Systems*. San Francisco, Morgan Kaufmann.
- Billings, C. E. (1991). "Human-centered aircraft automation: a concept and guidelines". *NASA Technical Memorandum*. Meffert Field, CA, USA, NASA Ames Research Center.
- Bizer, J., O. Günther, et al. (2006). "TAUCIS - Technikfolgenabschätzungsstudie Ubiquitäres Computing und Informationelle Selbstbestimmung". *B. f. B. u. Forschung*. Berlin, Germany, Humboldt University Berlin, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD).
- Bohn, J., V. Coroama, et al. (2004). "Living in a World of Smart Everyday Objects – Social, Economic, and Ethical Implications." *Journal of Human and Ecological Risk Assessment* 10(5): 763-785.
- Bose, I. and R. Pal (2005). "Auto-ID: Managing Anything, Anywhere, Anytime." *Communications of the ACM* 48(8): 100-106.

- Boyle, M. (2003). "A Shared Vocabulary for Privacy". 5th International Conference on Ubiquitous Computing, Seattle, Washington, USA.
- Brehm, J. W. (1966). *A Theory of Psychological Reactance*. New York, USA, Academic Press.
- Brown, S. A. and V. Venkatesh (2005). "Model of Adoption of Technology in Households: A Baseline Model Test and Extension Incorporating Household Life Cycle." *MIS Quarterly* 29(3): 339-426.
- Burger, J. M. (1989). "Negative reactions to increases in perceived personal control." *Journal of Personality and Social Psychology* 56(2): 246-256.
- Burrell, J., T. Brooke, et al. (2004). "Vineyard Computing: Sensor Networks in Agricultural Production." *IEEE Pervasive Magazine* 3(1): 38-45.
- Camenisch, J., A. Shelat, et al. (2005). "Privacy and Identity Management for Everyone". Workshop On Digital Identity Management (DIM), Fairfax, Virginia, USA.
- Capgemini (2005). "RFID and Consumers What European Consumers Think About Radio Frequency Identification and the Implications for Business". Surrey, Paris, Utrecht, Frankfurt.
- Center, E. P. I. (2004). "Proposed Guidelines For Use of RFID Technology: Enumerating the Rights and Duties of Consumers and Private Enterprises".
- Chen, S. C. and G. S. Dhillon (2003). "Interpreting Dimensions of Consumer Trust in E-Commerce." *Information Technology and Management* 4(2-3): 303-318.
- Chin, W. W. (1998). "The Partial Least Squares Approach to Structural Equation Modeling". in: *Modern Methods for Business Research*. Eds.: G. A. Marcoulides. Mahwah, NJ, USA, Lawrence Erlbaum Associates,; 295–336.
- Churchill, G. and D. Iacobucci (2001). *Marketing Research: Methodological Foundations*. Winfield, Kansas, USA, South-Western College Publications.
- Clee, M. A. and R. A. Wicklund (1980). "Consumer Behavior and Psychological Reactance." *Journal of Consumer Behaviour* 6(4): 389-405.
- Cohen, J. (1988). *Statistical Power Analysis for the behavioral sciences*. Hillsdale, NJ, USA, Lawrence Erlbaum Associates.
- Commission of the European Communities (2007). "Results of the Public Online Consultation on Future Radio Frequency Identification Technology Policy". Brussels, Belgium, European Commission.
- Compeau, D. R. and C. Higgins (1995). "Computer Self-Efficacy: Development of a Measure and Initial Test." *MIS Quarterly* 19(2): 189-211.
- Consolvo, S., Peter Roessler, et al. (2004). "Technology for Care Networks of Elders." *IEEE Pervasive Computing Magazine* 3(2): 22-29.
- Cornwell, J., I. Fette, et al. (2007). "User-Controllable Security and Privacy for Pervasive Computing". 8th IEEE Workshop on Mobile Computing Systems and Applications (HotMobile 2007), Tucson, Arizona, USA.
- Coutaz, J., J. L. Crowley, et al. (2005). "Context is Key." *Communications of the ACM* 48(3): 49-53.
- Cranor, L. F. (2003). "P3P: Making Privacy Policies More Useful". *IEEE Security & Privacy*. 1(6): 50-55.
- Cranor, L. F., B. Dobbs, et al. (2006). "The Platform for Privacy Preferences 1.1 (P3P1.1) Specification - W3C Working Group Note 13 November 2006." Electronic Source. Retrieved July 17th, 2007, 2007, from <http://www.w3.org/TR/P3P11/>.
- Cranor, L. F., P. Guduru, et al. (2006). "User Interfaces for Privacy Agents." *ACM Transactions on Computer-Human Interaction (TOCHI)* 13(2): 135 - 178
- Crites, S. L., L. R. Fabrigar, et al. (1994). "Measuring the affective and cognitive properties of attitudes: conceptual and methodological issues." *Personality and Social Psychology Bulletin* 20(6): 619-634.
- Csikzentmihalyi, M. (1990). *Flow: The Psychology of Optimal Experience*. New York., Harper Collins.

- Cunningham, M. (1967). "The Major Dimensions of Perceived Risk". in: Risk Taking and Information Handling in Consumer Behavior. Eds.: D. Cox. Cambridge, MA, USA, Harvard University Press.
- Davis, F. (1989). "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology." *MIS Quarterly* 13(3): 319-334.
- Davis, F., R. Bagozzi, et al. (1989). "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models." *Management Science* 35(8): 982-1003.
- Davis, F. and V. Venkatesh (2004). "Toward preprototyping user acceptance testing of new information systems: Implications for software project management." *IEEE Transactions on Engineering Management* 51(1): 319-346.
- Davis, F. R. (1989). "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology." *MIS Quarterly* 13(3): 319-340.
- deCharms, R. (1968). *Personal causation*. New York, Academic press.
- Derrett, N. (2006). "Is automation automatically a good thing?" *Personal and Ubiquitous Computing* 10(2-3): 56-59.
- Dey, A. and J. Mankoff (2005). "Designing Mediation for Context-Aware Applications." *ACM Transactions on Computer-Human Interaction* 12(1): 53-80.
- Diehl, K. (2005). "When Two Rights Make A Wrong: Searching Too Much in Ordered Environments." *Journal of Marketing Research* 42(3): 313-322.
- Diekmann, T., A. Melski, et al. (2007). "Data-on-Network vs. Data-on-Tag: Managing Data in Complex RFID Environments ". 40th Hawaii International Conference on System Sciences (HICSS-40), Waikolo, Hawaii, USA.
- Duce, H. (2003). "Public Policy: Understanding Public Opinion". A.-I. Center. Cambridge, USA, Auto-ID Center, Massachusetts Institute of Technology (MIT).
- Eagle, N. (2004). "Can Serendipity Be Planned?" *MIT Sloan Management Review* 46(1): 10-14.
- Encyclopaedia Britannica Micropedia (2005). "Control Systems". in: *Micropedia*. Eds. Chicago, London, New Delhi, Paris, Seoul, Sydney, Taipei, Tokyo, Encyclopaedia Britannica, Inc. 3: 589-590.
- Endsley, M. R. (1996). "Automation and Situation Awareness". in: *Automation and Human Performance - Theory and Application*. Eds.: R. Prasuraman and M. Mouloua. New Jersey, USA, Lawrence Erlbaum Associates: 163-181.
- Engberg, S., M. Harning, et al. (2004). "Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience". 2nd Annual Conference on Privacy, Security and Trust, New Brunswick, Canada.
- Engels, D., R. Rivest, et al. (2003). "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems". 1st International Conference on Security in Pervasive Computing, SPC 2003, Boppard, Germany.
- EPCglobal (2003). "900 MHz Class 0 Radio Frequency (RF) Identification Tag Specification".
- EPCglobal (2003). "EPCglobal Tag Data Standards Version 1.3". EPCglobal.
- EPCglobal (2005). "EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz - Version 1.0.9". Specification for RFID Air Interface. EPCglobal. Cambridge, Massachusetts, USA, EPCGlobal.
- EPCglobal (2007). "EPC Information Services (EPCIS) Version 1.0 Specification", EPCglobal.
- EPCglobal Inc. (2005, 31 January 2005). "EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz - Version 1.0.9." Specification for RFID Air Interface Electronic Source., from www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class1.pdf.
- Falter, M., O. Günther, et al. (2004). "Die Wahrnehmung von RFID in den Medien – Eine Inhaltsanalyse". *Arbeitsbericht*. Berlin, Germany, Humboldt-Universität zu Berlin, Institut für Wirtschaftsinformatik.
- Featherman, M. S. and P. A. Pavlou (2003). "Predicting e-services adoption: a perceived risk facets perspective." *International Journal of Human-Computer Studies* 59(4): 451-474.

- Federal Ministry of Economics and Technology, B. (2007). "European Policy Outlook RFID". Berlin, Germany, Federal Ministry of Economics and Technology.
- Feldhofer, M., S. Dominikus, et al. (2004). "Strong Authentication for RFID Systems Using the AES Algorithm". 6th Conference on Cryptographic Hardware and Embedded Systems (CHES 2004), Graz, Austria.
- Feldhofer, M. and C. Rechberger (2006). "A case against currently used hash functions in RFID protocols". Workshop on RFID Security (RFIDSec 06), Graz, Austria.
- Ferscha, A. (2007). "Pervasive Computing: connected > aware > smart". in: Die Informatisierung des Alltags - Leben in smarten Umgebungen. Eds.: F. Mattern. Berlin Heidelberg, Springer Verlag: 3-10.
- Fishbein, M. and I. Ajzen (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Reading, MA, USA, Addison-Wesley.
- Fiske, S. T. and S. E. Taylor (1991). *Social cognition*. New York, USA, McGraw-Hill.
- Fitts, P. M. (1951). *Human Engineering for an Effective Air-Navigation and Traffic-Control System*. Columbus, Ohio, USA.
- Floerkemeier, C., D. Anarkat, et al. (2003). "PML Core Specification 1.0". A.-I. Center. Cambridge, USA, Auto-ID Center, Massachusetts Institute of Technology (MIT).
- Floerkemeier, C. and R. Koh (2002). "Physical Mark-Up Language Update". A.-I. Center. Cambridge, USA, Auto-ID Center, Massachusetts Institute of Technology (MIT).
- Floerkemeier, C., R. Schneider, et al. (2004). "Scanning with a Purpose - Supporting the Fair Information Principles in RFID Protocols". in: *Ubiquitous Computing Systems*. Eds.: H. Murakami, H. Nakashima, H. Tokuda and M. Yasumura. Tokyo, Japan, Springer-Verlag.
- FoeBuD e.V. (2003, September 12th, 2007). "Positionspapier über den Gebrauch von RFID auf und in Konsumgütern." *Electronic Source*, from <http://www.foebud.org/rfid/positionspapier>.
- Fornell, C. and D. F. Larcker (1981). "Evaluating structural equation models with unobservable variables and measurement error." *Journal of Marketing Research* 18(1): 39–50.
- Friedman, B., I. E. Smith, et al. (2006). "Development of a Privacy Addendum for Open Source Licenses: Value Sensitive Design in Industry". 6th Conference on Ubiquitous Computing (Ubicomp), Irvine, CA, USA.
- Fusaro, R. (2004). "None of Our Business." *Harvard Business Review* 82(12): 33-44.
- Garfield, M. J. (2005). "Acceptance of Ubiquitous Computing." *Information Systems Journal* 22(4): 24-31.
- Garfinkel, S. and B. Rosenberg (2005). *RFID. Applications, Security, and Privacy*. New York, USA, Addison-Wesley Professional
- Gaver, B. and H. Martin (2000). "Alternatives: exploring information appliances through conceptual design proposals". *Conference on Human Factors in Computing Systems*, The Hague, The Netherlands.
- GCI, G. C. I. (2003). "Global Commerce Initiative EPC Roadmap". G. C. Initiative and IBM. Köln, GCI, Metro Gruppe, IBM Inc.
- Goffman, E. (1959). *The Presentation of Self in Everyday Life*. New York, USA, Doubleday.
- Grabner-Kräuter, S. and E. A. Kaluscha (2003). "Empirical research in on-line trust: a review and critical assessment." *International Journal of Human-Computer Studies* 58(6): 783–812.
- Greenwald, A. G. (1976). "Within-Subjects Designs: To Use or Not to Use " *Psychological Bulletin* 83(2): 314-320.
- Guenther, O. and S. Spiekermann (2005). "RFID and Perceived Control - The Consumer's View." *Communications of the ACM* 48(9): 73-76.
- Hackbarth, G., V. Grover, et al. (2003). "Computer playfulness and anxiety: positive and negative mediators of the system experience effect on perceived ease of use." *Information and Management* 40(3): 221 - 232
- Haselsteiner, E. and K. Breitfuß (2006). "Security in Near Field Communication (NFC)". *RFID Security 06*, Graz, Austria.

- Hassenzahl, M. (2001). "The Effect of Perceived Hedonic Quality on Product Appealingness." *International Journal of Human-Computer Interaction* 13(4): 481-499.
- Häuble, G. and V. Trifts (2000). "Consumer decision making in online shopping environments: the effects of interactive decision aids." *Marketing Science* 19(1): 4-21.
- Hayes, G. and K. N. Truong (2005). "Autism, Environmental Buffers, and Wearable Servers." *IEEE Pervasive Computing Magazine* 4(2): 14-17.
- Henderson, R. and M. Divett (2003). "Perceived usefulness, ease of use and electronic supermarket use." *International Journal of Human-Computer Studies* 59(3): 383-395.
- Hilty, L., C. Som, et al. (2004). "Assessing the Human, Social, and Environmental Risks of Pervasive Computing." *Human and Ecological Risk Assessment* 10(5): 853-874.
- Holman, R., S. John, et al. (2003). "Applying Video Sensor Networks to Nearshore Environment Monitoring." *IEEE Pervasive Computing Magazine* 2(4): 14-21.
- Horvitz, E., C. M. Kadie, et al. (2003). "Models of Attention in Computing and Communications: From Principles to Applications." *Communications of the ACM* 46(3): 52-59.
- Huberman, B., E. Adar, et al. (2004). "Valuating Privacy". *IEEE Security and Privacy*. 3(5): 22-25.
- Hui, K.-L., H. H. Teo, et al. (2007). "The Value of Privacy Assurance: An Exploratory Field Experiment." *MIS Quarterly* 31(1): 19-33.
- Hui, M. K. and J. G. Bateson (1991). "Perceived Control and the Effects of Crowding and Consumer Choice on the Service Experience." *Journal of Consumer Research* 18(2): 174-184.
- Inoue, S. and H. Yasuura (2004). "RFID Privacy Using User-controllable Uniqueness". *RFID Privacy Workshop, Massachusetts Institute of Technology (MIT), Cambridge, MA, USA*.
- Islam, N. and M. Fayad (2003). "Toward Ubiquitous Acceptance of Ubiquitous Computing." *Communications of the ACM* 46(2): 89-92.
- Jameson, A. and E. Schwarzkopf (2002). "Pros and Cons of Controllability: An Empirical Study". in: *Adaptive hypermedia and adaptive web-based systems: Proceedings of AH 2002*. Eds.: P. D. Bra, P. Brusilovsky and R. Conejo. Berlin Heidelberg, Springer Verlag: 193-202.
- Jannasch, U. and S. Spiekermann (2004). "RFID Technologie im Einzelhandel der Zukunft: Datenentstehung, Marketing Potentiale und Auswirkungen auf die Privatheit des Kunden". Berlin, Germany, Lehrstuhl für Wirtschaftsinformatik, Humboldt Universität zu Berlin.
- Jessup, L. M. and D. Robey (2002). "The Relevance of Social Issues in Ubiquitous Computing Environments." *Communications of the ACM* 45(12): 88-91.
- Juels, A., R. Rivest, et al. (2003). "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy". *10th ACM Conference on Computers and Communications Security (CCS 2003)*, Washington, USA.
- Juels, A., P. Syverson, et al. (2005). "High-Power Proxies for Enhancing RFID Privacy and Utility". *5th International Workshop on Privacy Enhancing Technologies (PET 2005)*, Cavtat, Croatia.
- Juels, A. and S. Weis (2005). "Authenticating Pervasive Devices with Human Protocols". *25th Annual International Cryptology Conference, Santa Barbara, California, USA*.
- Kantowitz, B. H. and R. Sorkin (1987). "Allocation of functions". in: *Handbook of Human Factors*. Eds.: G.-. Salvendy. New York, USA, Wiley: 365-369.
- Kaplan, L. B., S. G. J., et al. (1974). "Components of Perceived Risk in Product Purchase: A Cross-Validation." *Journal of Applied Psychology* 59(3): 287-291.
- Kassarjian, H. H. (1977). "Content Analysis in Consumer Research." *Journal of Consumer Research* 4(1): 8-18.
- Keller, I., W. van der Hoog, et al. (2004). "Gust of Me: Reconnecting Mother and Son." *IEEE Pervasive Computing Magazine* 3(1): 22-28.
- Keren, G. (1993). "Between- or Within-Subjects Design: A Methodological Dilemma". in: *A Handbook for Data Analysis in the Behavioural Sciences - Methodological Issues*. Eds.: G. Keren and C. Lewis. Hillsdale, New York, USA, Lawrence Erlbaum Associates: 257-27.

- King, W. R. and J. He (2006). "A meta-analysis of the technology acceptance model." *Information and Management* 43(6): 740-755.
- Klamer, L. (2005). "Kitchengate: The Screenfridge innovation — solutions to fulfil a need?" in: *ICT capabilities in action - What people do*. Eds.: L. Klamer, E. Mante-Meijer and J. Heres, European Co-operation in the field of Scientific and Technical Research (COST).
- Klayman, J. (1988). "Cue Discovery in Probabilistic Environments: Uncertainty and Experimentation." *Journal of Experimental Psychology Learning, Memory, and Cognition* 14(2): 317-330.
- Kobsa, A. (2007). "Privacy-Enhanced Personalization." *Communications of the ACM* 50(8): 24-33.
- Koehler, A. and C. Som (2005). "Effects of Pervasive Computing on Sustainable Development." *IEEE Technology and Society Magazine* 24(1): 15-23.
- Koufaris, M. (2002). "Applying the Technology Acceptance Model and Flow Theory to Online Consumer Behavior." *Information Systems Research* 13(2): 205-223.
- Krasnova, H. and E. Baran (2005). "Technology Paternalism". Institute of Information Systems, Berlin, Humboldt University Berlin.
- Krasnova, H., M. Rothensee, et al. (2007). "Perceived Usefulness of RFID-enabled Information Services – A Systematic Approach". *Wirtschaftsinformatik 2007 (WI'07)*, Karlsruhe, Germany.
- Krueger, R. A. (1994). *Focus Groups - A Practical Guide for Applied Research*. Thousand Oaks, Sage Publications.
- Kumar, V., D. Rus, et al. (2004). "Robot and Sensor Networks for First Responders." *IEEE Pervasive Computing Magazine* 3(4): 24-33.
- Lahlou, S., M. Langheinrich, et al. (2005). "Privacy and trust issues with invisible computers." *Communications of the ACM* 48(3): 59-60.
- Lange, S., A. Nonnengart, et al. (2002). "Benutzerbestimmbare Informationsflusskontrolle". *Sichere Software*. Saarbrücken, Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI).
- Langer, E. (1975). "The Illusion of Control." *Journal of Personality and Social Psychology* 32(2): 311-328.
- Langer, E. (1983). *The Psychology of Control*. Beverly Hills, USA, Sage Publications.
- Langer, E. (1989). *Mindfulness*. Reading, MA, USA, Addison-Wesley.
- Langer, E. and J. Rodin (1976). "The effects of choice and enhanced personal responsibility for the aged. A field experiment in an institutional setting." *Journal of Personality and Social Psychology* 34(2): 191-198.
- Lederer, S., J. Mankoff, et al. (2003). "Who Want to Know What When? Privacy Preference Determinants in Ubiquitous Computing". *International Conference on Human Factors in Computing Systems (CHI'2003)*, Ft. Lauderdale, Florida, USA.
- Lee, J. and N. Moray (1992). "Trust, control strategies and allocation of function in human-machine systems." *Ergonomics* 35(10): 1243-1270.
- Lehtonen, M., T. Staake, et al. (2006). "From Identification to Authentication - A Review of RFID Product Authentication Techniques". *Workshop on RFID Security 2006 (RFIDSec 06)*, Graz.
- Lipp, L. L. (2004). *Interaktion zwischen Mensch und Computer im Ubiquitous Computing*. Münster, LIT Verlag.
- Loewenstein, G. and D. Schkade (1999). "Wouldn't it be nice?: Predicting future feelings". in: *Well-being: The foundations of hedonic psychology*. Eds.: D. Kahneman, E. Diener and N. Schwarz. New York, Sage: 85-105.
- Lyman, S. M. and M. B. Scott (1967). "Territoriality: A neglected sociological dimension." *Social Problems* 15(2): 235-249.
- Lyytinen, K. and Y. Yoo (2002). "Issues and Challenges in Ubiquitous Computing." *Communications of the ACM* 45(12): 63-65.

- Lyytinen, K., Y. Yoo, et al. (2004). "Surfing the Next Wave: Design and Implementation Challenges of Ubiquitous Computing Environments." *Communication of the Association of Information Systems* 13: 697-716.
- Maes, P. and A. Wexelblat (1997). "Issues for Software Agent UI". MIT Media Lab. Cambridge, USA.
- Malhotra, Y. and D. F. Galletta (1999). "Extending the Technology Acceptance Model to Account for Social Influence: Theoretical Bases and Empirical Validation". 32nd Hawaii International Conference on System Science, Hawaii, USA.
- Margulis, S. (2003). "Privacy as a Social Issue and Behavioral Concept." *Journal of Social Issues* 59(2): 243-261.
- Mathieson, K. (1991). "Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior." *Information Systems Research* 2(3): 173-191.
- Mattern, F. (2001). "The Vision and Technical Foundations of Ubiquitous Computing." *UPGRADE, The European Online Magazine for the IT Professional* 2(5): 2-6.
- Mattern, F. (2007). *Die Informatisierung des Alltags - Leben in smarten Umgebungen*. Berlin Heidelberg, Springer Verlag.
- Mayer-Schönberger, V. (2007). "Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing". Cambridge, USA, Harvard University - John F. Kennedy School of Government.
- McFarlane, D. (1999). "Coordinating the Interruption of People in Human-Computer Interaction". *INTERACT 99*, Edinburgh, UK.
- McFarlane, D. (2002). "Comparison of four primary methods for coordinating the interruption of people in human-computer interaction." *Human-Computer Interaction* 17(1): 63-139.
- Mehrabian, A. and J. A. Russell (1974). *An Approach to Environmental Psychology*. Cambridge, MA, USA, MIT Press.
- Merrill, W. M., L. Girod, et al. (2004). "Dynamic Networking and Smart Sensing Enabled Next-Generation Landmines." *IEEE Pervasive Computing Magazine* 3(4): 84-90.
- Michahelles, F. and B. Schiele (2005). "Sensing and Monitoring Professional Skiers." *IEEE Pervasive Computing Magazine* 4(3): 40-46.
- Mick, D. G. and S. Fournier (1998). "Paradoxes of Technology: Consumer Cognizance, Emotions, and Coping Strategies." *Journal of Consumer Research* 25(9): 123-143.
- Molnar, D. and D. Wagner (2004). "Privacy and Security in Library RFID. Issues, Practices, and Architectures". 11th ACM Conference on Computer and Communications Security, Washington DC, USA.
- Myles, G., A. Friday, et al. (2003). "Preserving Privacy in Environments with Location-Based Applications". *IEEE Pervasive Computing*. 2(1): 56 - 64.
- Nakanishi, Y., K. Takahashi, et al. (2004). "iCAMS: A Mobile Communication Tool Using Location and Schedule Information." *IEEE Pervasive Computing Magazine* 3(1): 82-88.
- Nielsen, J. (1993). *Usability Engineering*. Mountain View, CA, USA, Morgan Kaufman.
- Nissenbaum, H. (1994). "Computing and Accountability." *Communications of the ACM* 37(1): 73-80.
- Norman, D. A. (1988). *The Psychology of Everyday Things*. New York, USA, Basic Books.
- Norman, D. A. (1998). *The Invisible Computer*. Cambridge, Massachusetts, USA, MIT Press.
- Norman, D. A. (2004). *Emotional Design - Why we love (or hate) everyday things*. New York, USA, Basic Books.
- Novak, T. P., D. L. Hoffman, et al. (2000). "Measuring the Customer Experience in Online Environments: A Structural Modeling Approach " *Marketing Science* 19(1): 22-42.
- Ohkubo, S., Kinoshita (2004). "Cryptographic Approach to "Privacy-Friendly" Tags". *RFID Privacy Workshop*, Massachusetts Institute of Technology, Cambridge, USA.
- Oliver Berthold and H. Federrath (2003). "Cookies tauschen - Profile vermischen." *Datenschutz und Datensicherheit DuD* 27(5).
- Orwell, G. (1949). 1984. New York, USA, The New American Library.

- Parasuraman, R. and M. Mouloua (1996). *Automation and Human Performance: Theory and Applications*. Hillsdale, NY, USA, Lawrence Erlbaum Associates.
- Parasuraman, R. and V. Riley (1997). "Humans and Automation: Use, Misuse, Disuse, Abuse." *Human Factors and Ergonomics Society* 39(2): 230-253.
- Parasuraman, R. and T. B. Sheridan (2000). "A Model for Types and Levels of Human Interaction with Automation." *IEEE Transactions on Systems, Man, and Cybernetics* 30(3): 286-297.
- Pater, H.-G. and P. Seidl (2007). "Der RFID-Markt aus Sicht der Anwender und Anbieter". in: *Internet der Dinge*. Eds.: H.-J. Bullinger and M. t. Hompel. Berlin Heidelberg New York, Springer: 19-38.
- Patrick, A. S., P. Briggs, et al. (2005). "Designing Systems That People Will Trust". in: *Security and Usability*. Eds.: L. F. Cranor and S. Garfinkel. Sebastopol, CA, USA, O'REILLY: 75-99.
- Pering, T., M. Sundar, et al. (2003). "Photographic authentication through untrusted terminals." *IEEE Pervasive Computing Magazine* 2(1): 30- 36.
- Peter, J. P. and M. J. Ryan (1976). "An investigation of perceived risk at the brand level." *Journal of Marketing Research* 13(2): 184-188.
- Peter, J. P. and L. X. S. Tarpey (1975). "A Consumer Analysis of Three Consumer Decision Strategies." *Journal of Consumer Research* 2(1): 29-37.
- Petty, R. E., D. T. Wegener, et al. (1998). "Attitudes and attitude change." *Annual Review of Psychology* 48: 609-648.
- Philipose, M., K. P. Fishkin, et al. (2004). "Inferring Activities from Interactions with Objects." *IEEE Pervasive Computing Magazine* 3(4): 50-57.
- Pierce, J. L., T. Kostova, et al. (2002). "The State of Psychological Ownership: Integrating and Extending a Century of Research." *Review of General Psychology* 7(1): 84-107.
- Pohl, H. (2004, June 8th, 2004). "Hintergrundinformationen der Gesellschaft für Informatik e.V. (GI) zu RFID - Radio Frequency Identification." *Electronic Source*. Retrieved September 12th, 2007, from <http://www.gi-ev.de/fileadmin/redaktion/Presse/RFID-GI040608.pdf>.
- Poulton, E. C. (1973). "Unwanted range effects from using within-subjects experimental designs." *Psychological Bulletin* 80(1): 113-121.
- Raento, M., A. Oulasvirta, et al. (2005). "ContextPhone: A Prototyping Platform for Context-Aware Mobile Applications." *IEEE Pervasive Computing Magazine* 4(2): 51-59.
- Renn, O. and M. M. Zwick (1997). *Risikoakzeptanz und Technikakzeptanz - Konzept Nachhaltigkeit* Berlin, Springer Verlag.
- Rieback, M. R., B. Crispo, et al. (2005). "Keep on Blockin' in the Free World: Personal Access Control for Low-Cost RFID Tags". 13th Security Protocol International Workshop, Cambridge, USA.
- Rieback, M. R., B. Crispo, et al. (2005). "RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management". 10th Australasian Conference on Information Security (ACISP 2005), Brisbane, Australia.
- Rieback, M. R., G. N. Gaydadjiev, et al. (2006). "A Platform for RFID Security and Privacy Administration". 20th Large Installation System Administration Conference (LISA'06), Washington D. C., USA.
- Rijsdijk, S. A. and E. J. Hultink (2003). "Honey, Have You Seen Our Hamster? Consumer Evaluations of Autonomous Domestic Products." *The Journal of Product Innovation Management* 20(3): 204-216.
- Riley, V. (1996). "Operator Reliance on Automation: Theory and Data". in: *Automation and Human Performance - Theory and Applications*. Eds.: R. Parasuraman and M. Mouloua. New Jersey, USA, Lawrence Erlbaum Associates: 19-35.
- Ringbauer, B. and E. Hofvenschiöld (2004). "Was macht es denn jetzt? Emotionale Faktoren bei der Akzeptanz von Smart Home Lösungen". *Usability Professionals 2004*, Stuttgart, Germany.
- Ringle, C. M., S. Wende, et al. (2005). "SmartPLS - Release 2.0". U. o. Hamburg. Hamburg, Germany.

- Rodin, J. (1990). "Control by any other name: Definitions, concepts and processes". in: Self-directedness: Cause and effects throughout the life course. Eds.: J. Rodin, C. Schooler and K. W. Schaie. Hillsdale, USA, Lawrence Erlbaum Associates: 1-15.
- Rogers, E. (2003). Diffusion of Innovations. New York, USA, The Free Press.
- Rohrmann, B. (1978). "Empirische Studien zur Entwicklung von Antwortskalen für die sozialwissenschaftliche Forschung." Zeitschrift für Sozialpsychologie 9: 222-245.
- Rosenthal, R. (1991). Meta-analytic procedures for social research. Newbury Park, Sage Publications.
- Rotter, J. B. (1954). Social learning and clinical psychology. Englewood Cliffs, Prentice Hall.
- Rowling, J. K. (2003). Harry Potter and the Order of the Phoenix. London, Bloomsbury.
- Satyanarayanan, M. (2002). "A Catalyst for Mobile and Ubiquitous Computing." IEEE Pervasive Computing Magazine 1(1): 2-5.
- Scerbo, M. W. (1996). "Theoretical Perspectives of Adaptive Automation". in: Automation and Human Performance. Eds.: R. Parasuraman and M. Mouloua. New Jersey, USA, Lawrence Erlbaum Associates: 37-63.
- Schmidt, A. (2000). "Implicit Human Computer Interaction Through Context." Personal Technologies 4(2-3): 191-199.
- Schmidt, A. (2007). "Eingebettete Interaktion - Symbiose von Mensch und Information". in: Die Informatisierung des Alltags - Leben in smarten Umgebungen. Eds.: F. Mattern. Heidelberg, Springer Verlag: 77-101.
- Schneier, B. (1999). "Attack Trees." Dr. Dobb's Journal 24(12): 21-29.
- Schoeman, F. D. (1984). Philosophical Dimensions of Privacy. Cambridge, UK, Cambridge University Press.
- Scholtz, J. and S. Consolvo (2004). "Towards a Discipline for Evaluating Ubiquitous Computing". I. Corporation, Intel Corporation.
- Schulzrinne, H., H. Tschofenig, et al. (2007, 18th August, 2007). "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information." Electronic Source. Retrieved 12th September, 2007, from <http://dret.net/biblio/reference/sch07>.
- Seligman, M. E. P. (1975). Helplessness: On Depression, development, and death. San Francisco, USA, Freeman.
- Sheeran, P. (2002). "Intention-behavior relations: A conceptual and empirical review". in: European Review of Social Psychology. Eds.: W. Stroebe and M. Hewstone. Chichester, UK, Wiley. 12: 1-36.
- Sheppard, B. H., J. Hartwick, et al. (1988). "The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research." Journal of Consumer Behaviour 15(3): 325-343.
- Sheridan, T. (2002). Humans and Automation: System Design and Research Issues. Santa Monica, USA, John Wiley & Sons.
- Sheridan, T. B. (1988). "Task allocation and supervisor control". in: Handbook of Human-Computer Interaction. Eds.: M. Helander. Amsterdam, The Netherlands, North-Holland: Elsevier Science Publisher: 159-173.
- Sheridan, T. B. (1996). "Speculations on Future Relations Between Humans and Automation". in: Automation and Human Performance - Theory and Applications. Eds.: R. Parasuraman and M. Mouloua. New Jersey, USA, Lawrence Erlbaum Associates: 449-460.
- Sheridan, T. B. (2000). "Function allocation: algorithm, alchemy or apostasy?" International Journal of Human-Computer Studies 52(2): 203-216.
- Sheridan, T. B. (2002). Humans and Automation: System Design and Research Issues. Santa Monica, John Wiley & Sons.
- Shi, Y., W. Xie, et al. (2003). "The Smart Classroom: Merging Technologies for Seamless Tele-Education." IEEE Pervasive Computing Magazine 2(2): 147-55.
- Sixsmith, A. and N. Johnson (2004). "A Smart Sensor to Detect the Falls of the Elderly." IEEE Pervasive Computing Magazine 3(2): 42-47.

- Skinner, E. (1996). "A Guide to Constructs of Control." *Journal of Personality and Social Psychology* 71(3): 549-570.
- Smith, J. H., S. Milberg, J., et al. (1996). "Information Privacy: Measuring Individuals' Concerns About Organizational Practices." *MIS Quarterly* 20(2): 167-196.
- Solove, D. J. (2006). "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154(3): 477-560.
- Spiekermann, S. (2001). "Online Information Search with Electronic Agents: Drivers, Impediments, and Privacy Issues". Institute of Information Systems. Berlin, Germany, Humboldt-Universität zu Berlin. Ph.D.: 312.
- Spiekermann, S. (2004). "EC Websites and Product Context: How Consumers' Product Focus drives their Navigational Needs". 5th ACM Conference on Electronic Commerce (EC'04), New York, USA.
- Spiekermann, S. (2007). "Privacy Enhancing Technologies for RFID in Retail- An Empirical Investigation". 9th International Conference on Ubiquitous Computing (UbiComp 2007), Innsbruck, Austria.
- Spiekermann, S. and O. Berthold (2004). "Maintaining privacy in RFID enabled environments - Proposal for a disable-model". in: *Privacy, Security and Trust within the Context of Pervasive Computing*. Eds.: P. Robinson, H. Vogt and W. Wagealla. Vienna, Austria, Springer Verlag. 780.
- Spiekermann, S. and L. F. Cranor (2007). "Engineering Privacy." in the review process.
- Spiekermann, S., J. Grossklags, et al. (2001). "E-privacy in 2nd generation E-Commerce". Proceedings of the 3rd ACM Conference on Electronic Commerce EC'01, Tampa, Florida, USA.
- Spiekermann, S. and F. Pallas (2005). "Technology Paternalism - Wider Implications of RFID and Sensor Networks." *Poesis & Praxis - International Journal of Ethics of Science and Technology Assessment* 4(1): 6-18.
- Spiekermann, S. and F. Pallas (2007). "Technologiepaternalismus – Soziale Auswirkungen des Ubiquitous Computing jenseits von Privatsphäre". in: *Die Informatisierung des Alltags. Leben in smarten Umgebungen*. Eds.: F. Mattern. Berlin Heidelberg New York, Springer: 311-325.
- Spiekermann, S., M. Strobel, et al. (2005). "Drivers and Impediments of Consumer Online Search: Self-controlled versus Agent-assisted Search". *Wirtschaftsinformatik*, Bamberg, Germany.
- Spiekermann, S. and H. Ziekow (2004). "Technische Analyse RFID-bezogener Angstsszenarien". Berlin, Germany, Institut für Wirtschaftsinformatik - Humboldt Universität zu Berlin: 44.
- Spiekermann, S. and H. Ziekow (2005). "RFID: a 7-point plan to ensure privacy". 13th European Conference on Information Systems (ECIS), Regensburg, Germany.
- Spiekermann, S. and H. Ziekow (2006). "RFID: A Systematic Analysis of Privacy Threats and a 7-Point Plan to Address Them." *Journal of Information System Security* 1(3): 2-17.
- Spinellis, D. D. (2003). "Position-Annotated Photographs: A Geotemporal Web." *IEEE Pervasive Computing Magazine* 2(2): 72-79.
- Stajano, F. (2003). "Location Privacy in Pervasive Computing". *IEEE Pervasive Computing*. 2(1): 46-55.
- Stanford, V. (2003). "Pervasive Computing Puts Food on the Table." *IEEE Pervasive Computing Magazine* 2(1): 13-18.
- Straub, D. W., M. Limayem, et al. (1995). "Measuring system usage: implications for IS theory testing." *Management Science* 41(8): 1328-1342.
- Streitz, N. A., C. Röcker, et al. (2005). "Designing Smart Artefacts for Smart Environments." *IEEE Computer* 38(3): 41-49.
- Taylor, S. and P. Todd (1995). "Understanding Information Technology Usage: A Test of Competing Models." *Information Systems Research* 6(2): 144-176.
- Te'eni, D., J. Carey, et al. (2007). *Human Computer Interaction - Developing Effective Organizational Information Systems*. New York, USA, John Wiley & Sons, Inc.

- Tennenhouse, D. (2000). "Proactive Computing." *Communications of the ACM* 43(5): 43-50.
- Thiesse, F. (2006). "Integration von RFID in die betriebliche IT-Landschaft." *Wirtschaftsinformatik* 48(3): 178-187.
- Thompson, S. C. and S. Spacapan (1991). "Perceptions of Control in Vulnerable Populations." *Journal of Social Issues* 47(4): 1-21.
- Tornatzky, L. G. and J. K. Katherine (1982). "Innovation Characteristics and Adoption-Implementation: A Meta-Analysis of Findings." *IEEE Transactions on Engineering Management* 29(1): 28-45.
- Tractinsky, N., A. S. Katz, et al. (2000). "What is beautiful is usable." *Interacting with Computers* 13: 127-145.
- Trafimow, D. and P. Sheeran (1998). "Some tests of the distinction between cognitive and affective beliefs." *Journal of Experimental Social Psychology* 34(4): 378-397.
- Trafimow, D., P. Sheeran, et al. (2002). "Evidence that perceived behavioural control is a multidimensional construct: Perceived control and perceived difficulty." *British Journal of Social Psychology* 41: 101-121.
- Triandis, H. C. (1977). *Interpersonal behavior*. Monterey, USA, Brooks/Cole.
- van Lieshout, M., L. Grossi, et al. (2007). "RFID Technologies: Emerging Issues, Challenges and Policy Options". I. Maghiros, P. Rotter and M. v. Lieshout. Luxembourg, European Commission, Directorate-General Joint Research Centre, Institute for Prospective Technological Studies.
- Várhelyi, A. (2002). "Speed management via in-car devices: effects, implications, perspectives." *Transportation* 29(3): 237-252.
- Varian, H. (1996). "Economic Aspects of Personal Privacy". *Privacy and Self-Regulation in the Information Age*. U. S. D. o. Commerce. Washington, USA.
- Venkatesh, V. (2000). "Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model." *Information Systems Research* 11(4): 342-365.
- Venkatesh, V. and F. Davis (2000). "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies." *Management Science* 46(2): 186-204.
- Venkatesh, V., M. G. Morris, et al. (2003). "User Acceptance of Information Technology: Toward a Unified View." *MIS Quarterly* 27(3): 425-478.
- VeriSign. (2004, January 1rst, 2004). "The EPC Network: Enhancing the Supply Chain." *Electronic Source*. Retrieved September 12th, 2007, from http://www.verisign.com/stellent/groups/public/documents/white_paper/002109.pdf.
- Vetere, F., M. R. Gibbs, et al. (2005). "Mediating intimacy: designing technologies to support strong-tie relationships". *Conference on Human Factors in Computing Systems (CHI 2005)*, Portland, Oregon, USA.
- Vlacic, L. (2001). *Intelligent vehicle technologies : theory and applications*. Oxford, Butterworth Heinemann.
- Vodafone (2003). "Vodafone Location Services - Privacy Management Code of Practice", Vodafone Ltd.
- Vroom, V. H. (1964). *Work and Motivation*. New Jersey, USA, John Wiley & Sons Inc.
- Wandke, H. (2005). "Assistance in human-machine interaction: a conceptual framework and a proposal for a taxonomy." *Theoretical Issues in Ergonomics Science* 6(2): 129-155.
- Ward, J. C. and J. W. Barnes (2001). "Control and affect: the influence of feeling in control of the retail environment on affect, involvement, attitude, and behavior." *Journal of Business Research* 54(1): 134-144.
- Warren, S. D. and L. D. Brandeis (1890). "The Right to Privacy." *Harvard Law Review* 4(5): 193-220.
- Weiser, M. (1991). "The Computer for the 21st Century." *Scientific American* 265(3): 94-104.
- Weiser, M. (1993). "Some Computer Science Issues in Ubiquitous Computing." *Communications of the ACM* 36(7): 75-84.

- Weiser, M. and J. S. Brown (1996). "The Coming Age of Calm Technology". Xerox Parc.
- Weiser, M. and J. S. Brown (1997). "The Coming Age of Calm Technology". in: Beyond calculation: the next fifty years. Eds. New York, USA, Copernicus: 75 - 85.
- Weiser, M., R. Gold, et al. (1999). "The origins of ubiquitous computing research at PARC in the late 1980s." IBM Systems Journal 38(4): 693-696.
- Weisz, J. R. and D. J. Stipek (1982). "Competence, contingency, and the development of perceived control." Human Development 25(4): 250-281.
- West, P. M., D. Ariely, et al. (1999). "Agents to the Rescue?" Marketing Letters 10(3): 285-300.
- Westin, A. (1967). Privacy and Freedom. New York, USA, Atheneum.
- White, R. W. (1959). "Motivation reconsidered: The concept of competence." Psychological Review 66: 297-333.
- Wickens, C. D. (1992). Engineering Psychology and Human Performance. New York, USA, HaberCollins.
- Wiener, E. L. and R. E. Curry (1980). "Flight-deck automation: promises and problems." Ergonomics 23(10): 995-1011.
- Wiener, N. (1948). Cybernetics - Or the Control and Communication in the Animal and the Machine Cambridge, MA, USA, MIT Press.
- Wijnalda, G., S. Pauws, et al. (2005). "A Personalized Music System for Motivation in Sport Performance." IEEE Pervasive Computing Magazine 4(3): 26-32.
- Woods, D. D. (1996). "Decomposing Automation: Apparent Simplicity, Real Complexity". in: Automation and Human Performance - Theory and Application. Eds.: R. Parasuraman and M. Mouloua. New Jersey, USA, Lawrence Erlbaum Associates: 3-17.
- Wu, J. H. and S.-C. Wang (2005). "What drives mobile commerce? An empirical evaluation of the revised TAM " Information and Management 42(5): 719-729.
- Yang, H.-d. and Y. Yoo (2004). "It's all about attitude: revisiting the technology acceptance model." Decision Support Systems 38(1): 19-31.
- Zhang, P. (2005). "The Importance of Affective Quality." Communications of the ACM 48(9): 105-108.
- Zhang, P. and N. Li (2005). "The Importance of Affective Quality." Communications of the ACM 48(9): 105-108.
- Zimbardo, P. G. and R. J. Gerrig (1996). Psychologie, Springer Verlag Berlin Heidelberg New York.

7

APPENDIX

APPENDICES

- APPENDIX 1:** Ubiquitous Computing Applications: A Snapshot from 2003 to 2006
- APPENDIX 2:** Experimental Stimulus for RFID PET Investigation: Films and Texts used in Study ① and Study ②
- APPENDIX 3:** Questionnaires used in Study ① and Study ②
- APPENDIX 4:** Scenario Descriptions used in the UC-AM Questionnaire on ‘The World of Tomorrow’
- APPENDIX 5:** Preparation Steps taken to carry out the Empirical Study for UC-AM on ‘The World of Tomorrow’
- APPENDIX 6:** PLS Output – Structural Equation Models of UC-AM
- APPENDIX 7:** Question Items used in the UC-AM Study on ‘The World of Tomorrow’
- APPENDIX 8:** Mean Valuation and Significance Tests for Control Group Variations made in order to detail the effects of UC-AM