

Perceived Control: Scales for Privacy in Ubiquitous Computing

Sarah Spiekermann¹

Humboldt University Berlin, Institute of Information Systems,
Spandauer Strasse 1, 14057 Berlin, Germany
sspiek@wiwi.hu-berlin.de

Abstract. Ubiquitous computing (UC) environments have triggered a strong research interest in privacy. How can people remain private when the infrastructure and objects around them begin to talk? Heading for an answer to this question many studies have rushed over past years to present guidelines for privacy-friendly UC design and have tempted even to rewrite the vocabulary of this socio-psychological construct. In doing so, most authors notice though that when it comes to requirements specification for privacy in UC, user-friendly technology design is really more about *perceived control* than it actually is about the end state of privacy itself. The current position statement therefore attempts to pull the two constructs –privacy and control- apart by theoretically reflecting on their mutual dependencies. It then proceeds by proposing a scale for appropriate measurement of perceived control in UC environments.

1 Introduction

Privacy is a construct widely investigated in the Information Systems world, both in the context of E-Commerce as well as in the context of UC. Except for a few articles what has been missing in IS research though is a thorough framing and defining of what privacy is including empirical testing of its building blocks based on properly defined scales. As a result of this lack of research, privacy definitions appear in different forms and facets, misconceptions not excluded. Consequently, when researching privacy for a Ubiquitous Computing context today, there is little common ground to build on.

Ubiquitous Computing refers to environments where most physical objects are enhanced with digital qualities. It implies “tiny, wirelessly interconnected computers that are embedded almost invisibly into just about any kind of everyday object” [1]. Thus, people buy and use products that can be automatically recognized, tracked, addressed and, potentially, trigger activities or services. Because of these properties, UC and especially one of its core technologies, RFID, have stirred some strong debates about privacy being at risk.¹

¹ RFID chips (tags) are embedded into the fabric of products and emit a unique product number once addressed by a reader. The reader feeds the number in a backend information

Yet, a misconception of privacy is actually articulated already in one of the most widely cited articles on Ubiquitous Computing, notably Mark Weiser's "The Computer for the 21st Century" [2]. Commenting on social challenges arising from UC, Weiser wrote: „The [social] problem [associated with UC], while often couched in terms of privacy, is really one of control." While Mark Weiser was right to point out that UC raises control issues reaching beyond privacy alone, it should be noted is that privacy has actually for decades been defined in terms of control. Altman [3] for example, one of the founding fathers of privacy research in the Western hemisphere, defined privacy in 1975 as "the selective control of access to the self or to one's group." Schoeman [4] saw privacy as "the control an individual has over information about himself or herself." And Margulis [5] 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." Summing up, privacy cannot be seen as separate from control. Instead it is deeply intertwined with it.

Unfortunately, IS research has seen few works building upon this fundamental insight.. For this reason, we want to investigate privacy more systematically with a view to its inherent control character. More specifically, we want to develop scales that are able to measure *perceived* privacy governance on the basis of perceived control. UC serves as the context in which privacy is sought.

2 Loss of Privacy through Loss of Control in UC

Loss of privacy in UC environments can really be due to two distinct reasons: The first one is relating to what we want to call '*people losing control over being accessed*'. In classical privacy literature, researchers relate to this aspect of privacy when they discuss the *collection* of data by marketers and other institutions [6]. For UC environments it is typically assumed that sensor- and RFID infrastructures will be ubiquitous. The so called "intelligent infrastructure" seeks to automatically adapt to people moving through space and for this it needs to establish connections with peoples' objects. People are envisaged to be read out by RFID readers or be tracked by other technologies. Building on Altman [3], Boyle refers to this privacy aspect in UC as the need "to control the *attention* of the UbiComp environments" [7]. This control can be exercised through Privacy Enhancing Technologies (PETs). PETs – according to current research – are supposed to enable users to protect themselves from being accessed against their will. First PETs for UC are blocker tags [8], the Privacy Awareness System (pawS) [9] or authentication based protection schemes [10-12].

The second factor impacting privacy in UC is due to a *lack of control over information use and maintenance* once people (or their objects) have been accessed. This concern about unauthorized secondary use is actually a historical one in privacy research [6]. However, UC adds a new dimension of relevance to this aspect of privacy since much more data is being collected. Ubiquitous multimedia

infrastructure where the nature of the product and potentially its owner is identified. Based on this information, further services are being triggered.

environments can, for example, lead to a more prevalent risk of disembodiment or disassociation as discussed by Belotti and Sellen [13]. Tracking of whereabouts and social network analysis suddenly gain a ‘physical’ dimension [14]. And, unique item identification inherent in new numbering standards, such as the Electronic Product Code (EPC) or IPv6 can lead to a degree of personal attribution and potential surveillance unseen before.

Still, this secondary use (and abuse) of information is not possible if there has not been access in the first place. This implies that controlling access is a crucial part of the privacy equation in UC. We therefore focus on the first dimension of privacy in UC: perceived control over the *access* that intelligent infrastructures may gain to individuals via their objects.

We proceed as follows: In section 3 we introduce the reader to the main theories of perceived control mostly deduced from the past 30 years of psychological research. Furthermore, we comment on two main privacy enhancing technologies envisioned to induce control over UC in people. Based on this, we then describe the development of scales that are able to measure control over UC perceived by PET users (section 4). We then apply these scales to a UC

3 Perceived Control and PETs in UC Environments

3.1. Perceived Control

Perceived control is a construct investigated in psychology since the 1960s [15]. One of the first investigations of control can be found in Seligman’s work on *learned helplessness* [16]. Learned helplessness was considered by Seligman as the opposite of being in control. Together with Abramson et al. [17] he defined helplessness as “cases in which the individual ... does not possess controlling responses” (p.51). People enter into a stage of numbness where they feel that their activity really does not impact the course of activities around them. In the context of UC this would imply that people have given up on protecting their privacy as they believe protection efforts to be in vain anyways.

Related to this feeling, but somewhat weaker in emotional strength is the notion of control as a means to achieve a desired outcome. Seligman propagated this aspect noting that “a person has control when a desired outcome’s occurrence is dependent on the person’s responses” [18]. In psychological research this position has mostly been referred to as *contingency* [19].

While Seligman and his peers’ research focused on response contingency, Langer propagated that people can only perceive control 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” [18]. In a UC environment this choice aspect would imply that people can opt easily out of being accessed by the intelligent infrastructure.

In order to recognize one’s choices a major requirement is that one is properly informed about one’s options. As Fiske and Taylor [20] put it: “...a sense of control

...is achieved when the self obtains or is provided with information about a noxious event” (p.201). Skinner calls this type of control “information control” [15]. In a UC context, *information control* would mean that people are not read out without them being aware of it.

Moreover, there is a *power* aspect in control that has been considered by Rodin writing: “[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” [21]. In fact, power is an important notion also in the literature on motivation. When people feel power they may be motivated to use a technology more rigorously.

Yet, Rodin also referred here to another notion of control which is one’s feeling of competence. If people do not feel competent enough to master a situation, they will not feel in control. Bandura is one of the scholars focusing on this aspect of control which is referred to as self-efficacy: “people’s beliefs about their capabilities to exercise control over events that affect their lives” [22]. Researchers in technology acceptance also use the term ‘*ease-of-use*’ in this context [23]. They see control as an important antecedent for peoples’ impression (or experience) to easily handle a new technology [24].

3.2. PETs for Perceived Control in UC

The goal of this article is to document the development of scales that are able to measure to what degree UC privacy enhancing technologies (PETs) are able to induce a perception of control in people. We assume that if people perceive control over UC environments through their PETs then they will also perceive themselves exercising their right to privacy. Before delving into the details of scale development yet it is important to describe available PETs for UC in more detail and to give the reader a perspective on the type of PETs used to test the control scales reported on hereafter.

Based on current UC PET research, we consider two types of privacy enhancing technologies as important in the context of RFID technology. We term these two alternative PET approaches the ‘user model’ and the ‘agent model’.

The *user model* implies that users exert full control over RFID tags by means of appropriate authentication mechanisms. Objects do not a priori respond to network requests. Instead the user self-initiates the use of intelligent services if they are available and useful in the respective context. The context decision when and how the use of tags is appropriate is thus taken by the object owner [10-12, 25]. If the owner of the object has some benefit from reviving an object’s RFID tag she can do so by authenticating access using a password. We expect the user model to induce a high level of control with users since the intelligent infrastructure cannot act autonomously.

In contrast, the *agent model* is based on the idea that RFID tags are left on active by default, thus always answering to network requests. Access control in this scenario is provided automatically via consumer privacy preferences that are residing in the network and are exchanged via some identity management system. This system takes the context-decision for the object owner when to answer network requests and when to deny them. When the network seeks access to a person (e.g. in order to send an

advertising message or track a person's movements), an identity management system, or agent, matches personal privacy preferences with claimed data collection purpose [9, 26]. Here, it is the an external party communicating with the agent that typically initiates communication. The user does not have to become active. The user trusts that his agent and the network interacting with it adhere to his privacy preferences.

4 Scale development and testing

4.1. Control Definition and Initial Item Development

Based on the control literature described in section 3.1. we developed scales that would be able to test peoples' perceived control over being accessed by an intelligent infrastructure. Helplessness, contingency, choice, power, information and ease-of-use described above served as the basic categories to frame the construct (see table 1).

Following the guidelines of proper scale development [27], the first step was the development of a proper definition of the perceived control construct. Based on an expert we formulated the following definition: "*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 the individual.*" We then developed 14 questions (items) capturing the different control categories identified above. To assess the relatedness of these items with the control construct definition we then conducted 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 categories that matched the different control aspects we had hoped to capture. Based on this ranking and classifying we were able to identify three questions that were the least related to the definition and we excluded them from further research. In parallel we adjusted four questions from the Technology Acceptance Model on ease-of-use to fit our context [23, 24]. The resulting 15 questions promised a high degree of content validity. Their importance ranking with regards to the control definition and their respective categories are presented in table 1. The next step was to test whether these categories would indeed show and be internally consistent when applied to UC PETs.

4.2. Empirical Item Testing

128 subjects were invited by a market research agency to participate in a study on tomorrow's shopping environments. They were demographically representative with 47% 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.

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. RFID technology,

representing the UC environment here, was explained neutrally. Its benefits and drawbacks were commented on without bias. 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 one piece of information: the privacy enhancing technology (the PET) available to the consumer to control his privacy. 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 so (user model). 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 purposes if the reading purpose would match a person's privacy preference (agent model).

Before and after seeing the film participants answered a battery of questions. The 15 control items were passed among other questions after the film. As depicted in table 1 they were answered on a 5-point Rohrman scale [28].

Table 1. Control items and categories

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

4.3. Internal Consistency and Reliability of Control Items

To understand whether the six control categories would really be reflected in the 15 control related questions we first conducted factor analysis. Assuming that there could be correlations between factors we chose oblimin rotation. Very few missing items were replaced by mean values. Principal component analysis was employed. Factor analysis was first conducted for group 1 (user model) and it was then analysed whether the results would replicate for group 2 (agent model). This first round of analysis showed that only 8 out of the 15 questions consistently (across both treatments) load on three factors with factor loadings above .6. 2 items, one ease-of-use question and one question on contingency saw low loadings for both treatments and were therefore eliminated from the item set. 5 remaining questions, notably those on power and choice would not load consistently on the three factors. In fact, for group 1 power and choice related questions loaded together with information and contingency items. Group 2 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 we opted to eliminate them from the list of questions, well recognizing that content validity of left over scales would suffer due to this step. The remaining 8 questions were used again to first run factor analysis for group1 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 (see table 2).

Table 2. Final factor loadings for the 2 PET treatments

Password PET (group 1)				Agent PET (group 2)			
	Pattern Matrix(a)				Pattern Matrix(a)		
	1	2	3		1	2	3
EUP 2	0,954	-0,048	-0,021	EUP 2	0,937	0,042	-0,028
EUP 1	0,881	-0,065	-0,094	EUP 1	0,925	-0,056	-0,045
EUP 3	0,854	0,162	0,088	EUP 3	0,905	0,047	0,074
IC 2	-0,114	0,918	-0,046	IC 2	-0,069	0,880	-0,024
IC 1	0,077	0,855	0,067	IC 1	0,026	0,872	0,004
CON 1	0,068	0,822	-0,025	CON 1	0,082	0,847	0,023
H 2	0,109	-0,014	0,905	H 2	0,062	-0,159	0,877
H 1	-0,165	0,001	0,800	H 1	-0,068	0,180	0,801

Rotation Method: Oblimin with Kaiser Normalization.
a. Rotation converged in 5 iterations.

Rotation Method: Oblimin with Kaiser Normalization.
a. Rotation converged in 4 iterations.

Factor 1 is clearly related to the category ‘ease-of-use’ of the PET. The three questions (EUP 1, 2, 3) measure to what extent one feels control over RFID, because one feels that the PET protecting one’s privacy is easy to use. Factor 3 is characterized by two highly loading items referring to ‘helplessness’ (H 1, 2). Factor 2 is characterized by the items classified as ‘information control’ as well as one question treating contingency (CON 1). Looking into the question text for the contingency item we can interpret the loading as respondents’ perception of their PET

as a means or channel information and then determine further steps. Consequently, we feel comfortable to regard factor 2 as a control dimension that measures to what extent one perceives control as a consequence of being informed.

Tables 3 and 4 show that the cumulative variance explained by these three factors is above 78% for both PET conditions. And, it is important to note that the three factors are almost not correlated. This means that they are measuring independent dimensions of perceived control.

The final step was to investigate the internal consistency of the three scales thus identified. For this purpose we calculated each item set's Cronbach α . The threshold of .8 was passed by the ease-of-use construct as well as the information control construct. The two items on helplessness displayed a rather weak Cronbach α of around .6. Potentially, these questions would need to be retested in future research and be complemented with other items to form a better scale.

Table 3. Control scales group 1 (Password), reliability statistics

Control scales	Item	Cron α	Culm. Variance explained	Corr (r)	Corr (r)	Corr (r)
Ease-of-use of the PET	EUP 1	.881	38,33%	.243	.110	-.214
	EUP 2					
	EUP 3					
Information Control	CON 1	.837	64,30%			
	IC 1					
	IC 2					
Helplessness	H 1	.650	78,63%			
	H2					

Table 4. Control scales group 2 (Agent), reliability statistics

Control scales	Item # item rank	Cron α	Culm. Variance explained	Corr (r)	Corr (r)	Corr (r)
Ease-of-use of the PET	EUP 1	.915	34,70%	.092	.118	.050
	EUP 2					
	EUP 3					
Information Control	CON 1	.836	61,91%			
	IC 1					
	IC 2					
Helplessness	H 1	.579	78,99%			
	H2					

5 Applying Control Scales to UC PETs

Typically, scales identified on the basis of one sample should not be applied to the same sample for the report of actual findings. Still, in order to add practical meaning

to the control scales discussed in this article, we want to apply them here to demonstrate their usefulness.

As outlined above, we want to use the scales to measure peoples' perceived control over UC technology once they have a PET to protect their privacy. Thus, we want to measure how people perceive exercising privacy with the help of a PET. As described in section 4.2. 128 subjects answered to the control scales described above upon seeing a film on RFID deployments in retail and at home. Group 1 and 2, however, differed with respect to the PET displayed to them in the film stimulus. With this experimental set-up it became possible to test whether people perceive different levels of control depending on the type of PET used. Recall that in the user model, people would get immediate control over when to access the intelligent infrastructure. Only upon reception of a personal password the intelligent infrastructure would be able to read out peoples' RFID chips. On the other hand, the agent model proposed a PET residing on a mobile network and operating automatically on the basis of privacy preferences specified in advance of transactions. Here, control would be delegated to an agent. The hypothesis we had upon designing the experiment was that participating subjects would perceive more control in the user model and less control in the agent model. Thus, producing an argument for more research efforts in UC technology designs putting control physically into peoples' hands.

Peoples' perception of control on the basis of having one of the two PETs at their disposition is displayed in table 5. It turns out that – against expectations- perceived control is similar for both PET technologies. More specifically, people report to feel helpless (out of control) no matter what PET is at hand. This is despite the fact that they consider both PETs to be rather easy to use. The degree to which they feel informed to actively control the environment is judged on as medium. The mean control judgements indicate that the password scheme may be slightly easier to use, but this difference is statistically non significant. The conclusion that can be drawn from these results is that *no* PET presented to participants in the current study seems to induce in people a perception of control. The proposal of either PET solution must be questioned seen that people do not feel in control with any one of the two and may therefore question the ability to effectively protect their privacy with them.

6 Conclusion

The current article documents the development of three scales that are able to measure peoples' perception of control over being accessed when moving in UC environments and having a PET to protect their privacy. Control is measured with a view to whether people feel informed and are able to use the PET. Furthermore, loss of control is considered by the degree of helplessness perceived by users. When researchers of UC conceive technologies today that impacts peoples' privacy, they may want to test whether the environments they envision induce a positive feeling of control. The scales presented here, may serve this purpose. Especially the two factors relating to ease-of-use and information control could be used as design guidelines for UC developers.

Applying the control scales to two PET scenarios envisioned by UC scholars show that both of them do not win peoples' trust. More precisely, they do not induce a feeling of control and thus privacy. Since they are broadly the most prevalent PET options for RFID technology thought of today, this may cause designers of RFID technology to potentially rethink the marketability of the privacy processes they currently envision.

Table 5. Control scales and mean answers applied to two UC PETs

Control Scale	Questions (1=fully agree, 5=do not agree at all)	mean (user model)	mean (agent model)
Ease-of-use of the PET	To learn to use <the PET> would be easy for me.	1.65	2.02
	It would be easy for me to learn skillful use of <the PET>. ¹⁾	1.92	2.15
	I find <the PET> easy to use.	2.16	2.44
Information Control	Using <the PET> I would always know when and by whom I have been read out.	2.96	2.85
	Through <the PET> I would always be informed of whether and how the intelligent environment recognizes me.	2.72	2.51
	Thanks to <the PET> I could determine myself whether or not I'll interact with the intelligent environment.	2.49	2.44
Helplessness	I could imagine that if the intelligent environment set out to scan me, it would be able to do so despite <the PET>.	1.57	1.53
	Eventually <the PET> will not be able to effectively protect me from being read by the intelligent environment.>	1.92	1.78

6 References

- [1] F. Mattern, "The Vision and Technical Foundations of Ubiquitous Computing," *Upgrade*, vol. 2, pp. 2-6, 2001.
- [2] M. Weiser, "The Computer for the 21st Century," in *Scientific American*, vol. 265, 1991, pp. 94-104.
- [3] I. Altman, *The environment and social behavior: Privacy, personal space, territory, crowding*. Monterey, California: Brooks/Cole, 1975.
- [4] F. Schoeman, *Philosophical Dimensions of Privacy*. Cambridge, UK: Cambridge University Press, 1984.
- [5] S. Margulis, "Privacy as a Social Issue and Behavioral Concept," *Journal of Social Issues*, vol. 59, pp. 243-261, 2003.

- [6] J. H. Smith, S. Milberg, J., and S. Burke, J., "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly*, vol. 20, pp. 167-196, 1996.
- [7] M. Boyle, "A Shared Vocabulary for Privacy," presented at Fifth International Conference on Ubiquitous Computing, Seattle, Washington, 2003.
- [8] A. Juels, R. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," presented at 10th Annual ACM CCS 2003, 2003.
- [9] M. Langheinrich, "A Privacy Awareness System for Ubiquitous Computing Environments," presented at 4th International Conference on Ubiquitous Computing, UbiComp2002, Göteborg, Sweden, 2003.
- [10] D. Engels, R. Rivest, S. Sarma, and S. Weis, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," presented at First International Conference on Security in Pervasive Computing, SPC 2003, Boppard, USA, 2003.
- [11] S. Engberg, M. Harning, and C. Damsgaard Jensen, "Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience," presented at Second Annual Conference on Privacy, Security and Trust, New Brunswick, Canada, 2004.
- [12] S. Spiekermann and O. Berthold, "Maintaining privacy in RFID enabled environments - Proposal for a disable-model," in *Privacy, Security and Trust within the Context of Pervasive Computing*, vol. 780, *The Kluwer International Series in Engineering and Computer Science*, P. Robinson, H. Vogt, and W. Wagealla, Eds. Vienna, Austria: Springer Verlag, 2004.
- [13] V. Bellotti and A. Sellen, "Design for Privacy in Ubiquitous Computing Environments," presented at 3rd European Conference on Computer Supported Cooperative Work ECSCW'93, Milan, Italy, 1993.
- [14] S. Spiekermann and H. Ziekow, "RFID: a 7-point plan to ensure privacy," presented at 13th European Conference on Information Systems (ECIS), Regensburg, 2005.
- [15] E. Skinner, "A Guide to Constructs of Control," *Journal of Personality and Social Psychology*, vol. 71, pp. 549-570, 1996.
- [16] M. E. P. Seligman, *Helplessness: On Depression, development, and death*. San Francisco: Freeman, 1975.
- [17] L. Y. Abramson, M. E. P. Seligman, and J. D. Teasdale, "Learned helplessness in humans," *Journal of Abnormal Psychology*, vol. 87, pp. 49-74, 1978.
- [18] E. Langer, *The Psychology of Control*. Beverly Hills: Sage Publications, 1983.
- [19] H. Heckhausen, *Motivation and Action*. Berlin: Springer Verlag, 1991.
- [20] S. Fiske and S. Taylor, *Social cognition*. New York: McGraw-Hill, 1991.
- [21] J. Rodin, "Control by any other name: Definitions, concepts and processes," in *Self-directedness: Cause and effects throughout the life course*, J. Rodin, C. Schooler, and K. W. Schaie, Eds. Hillsdale: Erlbaum, 1990, pp. 1-15.
- [22] A. Bandura, "Human agency in social cognitive theory," *American Psychologist*, vol. 44, pp. 1175-1184, 1989.
- [23] F. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*, vol. 13, pp. 319-348, 1989.
- [24] V. Venkatesh, "Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model," *Information Systems Research*, vol. 11, pp. 342-365, 2000.
- [25] Y. Inoue, "RFID Privacy Using User-controllable Uniqueness," presented at RFID Privacy Workshop, Massachusetts Institute of Technology, Cambridge, MA, USA, 2004.
- [26] C. Floerkemeier, R. Schneider, and M. Langheinrich, "Scanning with a Purpose - Supporting the Fair Information Principles in RFID Protocols," presented at 2nd International Symposium on Ubiquitous Computing Systems, Tokyo, Japan, 2004.

- [27] G. Churchill and D. Iacobucci, *Marketing Research: Methodological Foundations*: South-Western College Pub, 2001.
- [28] B. Rohrmann, "Empirische Studien zur Entwicklung von Antwortskalen für die sozialwissenschaftliche Forschung," *Zeitschrift für Sozialpsychologie*, vol. 9, pp. 222-245, 1978.