Privacy and Security in Technology-enhanced Environments: Exploring Users' Knowledge about Technological Processes of Diverse User Groups

Oliver Sack[1,*], Carsten Röcker[2]

[1]Department of Psychology, RWTH Aachen University, Jaegerstraße 17-19, Aachen 52066, Germany
[2]Human-Computer Interaction Center (HCIC), Theaterplatz 14, Aachen 52056, Germany
*Corresponding Author: oliver.sack@psych.rwth-aachen.de

Abstract   This article reports on two user studies exploring the knowledge of end users about technical processes of technology-enhanced home environments, which are often assumed to play an important role for attitudes such as privacy and security. In the first study (n=12 participants between 19-71 years of age), we analyzed user knowledge about technical processes using the teach-back methodology. In the second study, we additionally applied new developed questionnaires and analyzed participants' data (n=24 participants between 19-76 years of age) regarding relations of user factors, users' knowledge about technical processes and attitudes such as privacy and security of technology-enhanced environments. In contrast to existing assumptions, the results showed that general structural knowledge about technical processes was not related with attitudes such as privacy and security. Additionally, we found that most participants had only relatively superficial knowledge about technical processes, which was further influenced by age and technology experience.

Keywords   Technology-enhanced Environment, Ambient Assisted Living, Mental Model, Teach Back, Privacy, Security

1. Introduction

Increasing life expectancies and decreasing birthrates in most industrialized countries [1] lead to a constantly growing interest in technology-enhanced environments for providing medical services. These new technical solutions gain more and more importance for enabling elderly people with inferior health to live a mostly independent and self-paced life [2,3]. Generally, technology-enhanced environments combine information, communication and medical engineering technologies [4] to provide a wide range of healthcare concepts for supporting and assisting people in their everyday life [5], e.g., monitoring of vital parameters via wireless technologies in the living room. But they do not only offer assistance in sustaining autonomy and quality of life of older adults [2]. They are more beneficial in the long run by limiting the costs of medical care [6].

However, as technology-enhanced environments are using technologies that can record (sensing) and save data (memory) everywhere and at anytime (ubiquity) without the monitored person noticing it (invisibility), privacy and security concerns occur, resulting in tendencies of refusing to participate in such systems [7-9]. Weiser, Gold, and Brown [9] phrased it like this: "If the computational system is invisible as well as extensive, it becomes hard to know what is controlling what, what is connected to what, where information is flowing, how it is being used, (…) and what the consequences are of any given action" (pp. 2-3). Considering these potential privacy and security concerns it is crucial to gain broader insights into underlying determinants by analyzing the mental models of individual users.

According to Johnson and Henderson [10] mental models can be defined as "the users' high-level understanding of how the technical application works; it allows the user to predict what the application will do in response to various user-actions" (p. 21). Mental models are influenced by a variety of factors. In this article, we will especially focus on *technology experience* and *age*. Already Piaget's concept of assimilation and accommodation shows that mental models are modified through experience [11]. People use preexisting experiences to build an understanding of new constructs. This implies that, if the experience with an technology-enhanced home environment cannot be assimilated into an existing mental model, users have to accommodate their mental models to the new concept of technology-enhanced home environments [11]. The assumption that mental models are influenced by prior experience is backed by Norman [12], who explained that mental models are created through a "user's technical background, previous experience with similar systems, and the structure of the human information processing system" (p.

8). Beside the influence of preexisting experience with technologies, also age is likely to have an influence on mental models. Calero-Valdez, Ziefle, Alagöz, and Holzinger [13] studied spatial representation of mobile device menu structures. They found that beside technical experience, age was a relevant factor influencing the appropriateness of these mental representations. Although spatial representations are not directly relevant for the research questions addressed in this article, it is noteworthy that technical experience decreases with higher age [14]. Therefore, we expect that the accuracy of mental models might decrease due to the age-related decrease of technical experience.

This leads to the question of the connection between users' knowledge about technical processes and attitudes such as privacy and security. Focusing on privacy, we know that "people report to be very sensitive and critical whenever mobile technology or smart medical technology enters their homes" ([15], p. 414), for example, using microphones in bedrooms and bathrooms is perceived as a strong violation of privacy [16]. With regard to personal medical records, the National Consumer Health Privacy Survey [17] found that 67% of consumers in California are concerned about their medical privacy, and users might not use technologies, which they perceive as a threat of privacy [7,2]. This shows that users care about their privacy. Nevertheless, users are often not aware of possible privacy violations when using specific technologies. This was demonstrated by Kaasinen [18] in a study with location-aware mobile devices. Results showed that users leave their privacy protection completely to "service providers and policy-makers" ([18], p. 78). In addition, participants were mostly not aware of the fact that they could be tracked when using location-aware services. Here inferior knowledge (associated with a less appropriate mental model) about the technology results in lower privacy concerns. Ina study on the relation between users' knowledge of online credit-card transaction and privacy, Acquisti and Grossklags [19] reported "evidence of simplified mental models" (p. 6), which lead them to the conclusion that "consumers often lack enough information to make privacy-sensitive decisions" (p. 1).

However, not only the decision about privacy is guided by mental models, existing literature (e.g., [20], 2010) also shows that *security* concerns are influenced by mental models. Especially knowledge of computer security as a mental model might affect the perception of security: "Many users try to avoid making security decisions because they feel they don't have the knowledge and skills to maintain proper security" ([21], p. 57). Consequently, security decisions are likely to be influenced by mental models [20]. Asgharpour, Liu, and Camp [22] showed that a higher degree of knowledge of security mechanisms of computers is associated with a more reliable prediction and anticipation of "computer security violations" (p. 368).
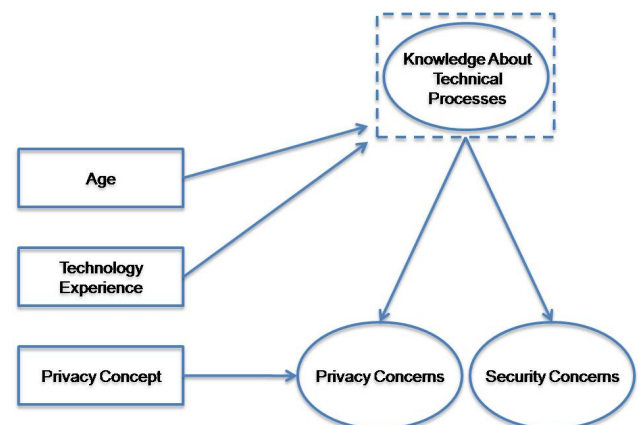
Summing up these findings leads to the assumption that more appropriate mental models (represented as a higher concurrence between the actual computational processes and the users' knowledge about these computational processes in technology-enhanced home environments) might influence the perception of privacy and security in such systems. In this context, it is important to notice that technology-enhanced home environments include a multitude of complex and highly interconnected system components and therefore offer numerous possibilities for potential privacy and security violations. Following our argumentation above, we assume that users with less technical knowledge are *unaware* of many possible violations of their personal privacy and security. In contrast, users with more appropriate mental models might have higher privacy and security concerns, as they are *aware* of the consequences of potential system malfunctions.

2. Research Approach

As illustrated above privacy and security attitudes are likely to be influenced by the mental models (represented as knowledge about technical processes). Until today, little is known about users' knowledge about technical processes in technology-enhanced environments, although this is a critical factor in the decision making process of a user. Hence, it is important to understand users' knowledge about technical processes as it plays an important role for forming personal attitudes such as privacy and security. This also includes a profound understanding of the relation of individual user characteristics as a source of mental models.

This article therefore analyzes (a) users' knowledge of technical processes in technology-enhanced environments, (b) the relation between these knowledge structures and different user characteristics, and (c) the influence of technical knowledge on privacy and security attitudes. Figure 1 shows the conceptual model underlying our research.

Figure 1. Research model (independent variables are shown in rectangular, dependent variables in elliptic shapes).

3. Methodology

In order to answer the research questions illustrated above, two constitutive studies have been conducted:

(1) First, we explored prevalent mental models by analyzing the individual user knowledge about technical processes in technology-enhanced home environments. The results gained in this study also contributed to the development of an assessment method for knowledge structures.

(2) In the second study, we first verified our previous findings and then related technical knowledge to user characteristics as well as privacy and security attitudes.

3.1. Material

Considering the fact that mental models emerge best by feeling and actively experiencing a technical system [10,23], all studies were conducted in the *Future Care Lab* (Figure 2), a simulated intelligent home environment at RWTH Aachen University. The lab provides a full-scale technical infrastructure and includes several mobile and stationary devices. It thereby allows studying users of different ages and with different health backgrounds in realistic usage situations [24]. In order to investigate how participants understand computational processes in technology-enhanced home environments we used a fully integrated personal assistance system for heart patients, which was developed within the project "eHealth – Enhancing Mobility with Aging" [25]. The system was specifically designed for enabling elderly and chronically ill patients to maintain their mobility and independence.

Figure 2. Future Care Lab. The interactive wall-sized display is shown on the left side. ((c) Kai Kasugai, eHealth Group RWTH Aachen University).

Conceptually, the system comprises three main components: the *sensor unit*, the *middleware unit* and the *actor unit*. In our situation, the sensor unit consisted of two medical sensors (Figure 3).

First, a standard sphygmomanometer with an inflatable cuff (Boso, Jungingen, Germany) was used to measure blood pressure and heart rate. The device was wired to the system's middleware unit. For automated weight monitoring, a digital scale was used (Kern, Balingen, Germany), which was integrated into the floor in front of the display wall. The scale was also wired the middleware unit.

((c) Kai Kasugai, eHealth Group RWTH Aachen University) and scale integrated into the floor (right).
Figure 3. Sphygmomanometer embedded in a coffee table (left)

Analog-to-Digital Converters (ADC) transformed analog sensor signals to a digital data stream, which was then transferred to the middleware unit**.** The software architecture of the middleware was based on the Open Service Gateway initiative framework (OSGi), which facilitates interoperability of various input devices. It would have been possible to store collected data and to get access from an online database. A feature-extracting software structured the data and extracted relevant user-centered information [26]. The actor unit displayed relevant user information, e.g., graphical summaries of different vital parameters. Technically, it would have been possible that the graphical output is accessed and interpreted by a specialist in a remote heart center. For further information about the technical implementation please see [27], [26] or [28].

3.2. First Study

In order to explore prevalent knowledge structures we invited 12 participants ($N_{1.1...1.12}$, aged from 19-71, balanced to age and gender) into the Future Care Lab, where they experienced and interacted with various systems. Most of the older adults participating were active part of their workforce and could be noted as quite healthy. Each participant was asked to operate a home-monitoring application originally designed for patients suffering from serious heart failures. After answering a pretest questionnaire, which contained questions regarding different user characteristics, the experimenter demonstrated how to measure one's own weight and blood pressure. In the next step, the experimenter explained how to navigate through the graphical measurement menu of the wall-sized display (Figure 4). The participants then executed the previously illustrated steps on their own.

Figure 4. Participant navigating through the graphical overview of vital parameters.

After having tried the application, the participants were asked to describe the system using the teach-back method. With its hermeneutic approach [29] it gave us the possibility to extract users' knowledge about technical processes. The method has been applied in different technological contexts, e.g. spreadsheet application [30] or in the domain of physics [31]. The participants were instructed to explain everything in depth to the interviewer, as if the interviewer was a student [29]. Participants were motivated to answer in a way, they felt most comfortable with (e.g., drawing, writing, speaking or a combination of these). We used two often applied types of questions within this technique: the *what is?*-type and the *how to?*-type. The first type relates to conceptual and semantic knowledge. The second type provides the possibility to explore the procedural knowledge a user has about the system [29].

In order to familiarize participants with the teach-back method the experimenter carefully described the teach-back procedure and the purpose of extracting mental models of how the previously experienced system might work. It was of great importance to get a detailed response of each participant. Therefore, the experimenter instructed and encouraged each participant to answer explicitly and completely. We noted that there were no right or wrong answers [31]. To motivate participants to share their knowledge with the experimenter, subjects were instructed "that the 'learner' [i.e. the interviewer] does not know anything about the system" ([30], p. 141). After introducing the methodology participants were asked to answer questions related to privacy and security: "*Explain…how data is transferred from the blood pressure monitor to the system.*" (Q1), "*Explain…how data is transferred from the scale to system."* (Q2) and "*Explain…how data is transferred from the system to your physician.*" (Q3).

In addition, we interviewed three experts, who were involved in the development of the laboratory. By interviewing experts we expected to specify system details specifically relevant for users (Figure 5). This was helpful to calculate the degree of congruence between the participants' mental models and the *conceptual model*. According to Johnson and Henderson [10] we extracted a best answer of experts. Therefore, three experts of different academic fields (engineering, architecture and computer science) were asked to participate in the study.

All interviews were conducted in German and audio-recorded for transcription. Quotations provided in this article were later translated to English. Before running the study, the script was tested with users in three pre-tests. Each session took between 40 and 50 minutes.

First results showed gaps of knowledge about technical processes, which is congruent with the assumption of Acquisti and Grossklags [19] that users have "simplified mental models" (p. 6). A lower degree of accuracy seemed to be more a result of incomplete answers rather than incorrect knowledge. For instance, users did not mention how data is converted. Nevertheless, if a user made a wrong assumption about the system, this was mostly related to how data is

transferred from the blood pressure monitor to the system, e.g., via WLAN or Bluetooth, despite the fact that a data transmission cable was visibly connected to the blood pressure meter. Additionally, the first study helped to improve the knowledge assessment for the main study. In order to analyze the influence of mental models on attitudes, it is necessary to investigate other factors (e.g., privacy attitudes), which might have an influence, in more detail. In this context, we assume that participants transfer their general privacy concept to the perception of privacy in the technology-enhanced environments.
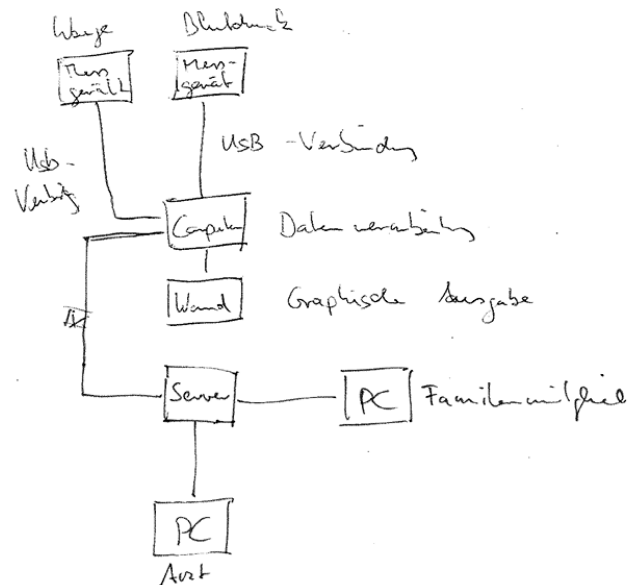

Figure 5.   An expert's drawing of computational processes referring to Q1, Q2 and Q3.

3.3. Second Study

3.3.1. Procedure

The main evaluation builds on the first study described above and uses the same test application and components. Hence, we refrain from a detailed description of the procedure and test material. Compared to the first study, we explicitly aimed at capturing user characteristics in more detail by using more comprehensive pretest and posttest questionnaires. Each user session consisted of four main parts:

a) Pretest Questionnaire. In the pretest questionnaire we collected individual characteristics such as age, gender, educational level, profession, subjective technical self-confidence (STC) [31], users' general privacy concepts [33,34], general technology experience [35,36]. Additionally we directly assessed participants' experience with information and communication technologies (ICT) (e.g., smart phone) as well as assistive medical devices (MedTech) (e.g., sphygmomanometer). For both types of technology, usage-frequency had to be rated on a 6-point Likert-scale from 1 (*daily*) to 6 (*never*) and perceived ease-of-use was

assessed on a 6-point Likert-scale (1=*very easy* and 6=*very difficult*), as well. Finally, TE$_{ICT}$ and TE$_{MedTech}$ were summed using usage frequency and perceived ease-of-use. Scores are expressed as percentages.

b) Home-Monitoring Situation. In the second part participants ran the home-monitoring situation, which was guided by the procedure of the first study.

c) Posttest Questionnaire. After running the situation each participant answered a posttest questionnaire, which focused on attitudes regarding technology-enhanced home environments. Participants were asked to rate bipolar statements referring to their attitudes such as privacy (e.g., "The home monitoring system limits my privacy") and security (e.g., "It is likely that my data transfer is not sufficiently protected to third parties") [2]. Continuous rating scales we used to capture the level of agreement with different statements (e.g., left side="I would have to control, if and what data is collected by the system" to right side="I wouldn't have to control, if and what data is collected by the system"). Each pair of contradicting statements was considered as an item. Rating scales were designed to be exactly 10cm long. Both statements marked the endpoints of a 10-point scale and referred to *1* and *10*. For instance, if a participant gave a value of *1* in the previous question, the participant would definitely need to control, if and what data is collected. Completing the posttest questionnaire took 15-20 minutes,

d) Interview. The framework of the teach-back method was already successfully applied in the first study to get participants to speak and to assess their knowledge about technical processes. As the method delivered valuable insights in the first study, we used the same approach for the interviews conducted in the main study. Participants had to answer the question, how data is transferred from the system to their physician. This question was considered to cover a wide range of technical aspects.

Both, pretest and posttest questionnaires were validated by linguistic experts with respect to comprehensibility and wording. The entire session had a duration of 40 minutes in total.

3.3.2. Variables

As we will see in a later step of analysis some variables have an intervening role as predictor and criteria. To avoid confusion in the first step of the analysis we use individual user factors as independent variables.

Independent Variables

Age. Especially older adults from the services, which technology-enhanced home environments provide. Therefore, the participants' age was the first independent variable, as we expected age-related decreases of technical experience might have an influence on the accuracy of the mental models. However we take into account that age is an "indicator of other critical variables, which might be carried by age" ([35], p. 316).

Technology Experience (TE). Technical experience is a broad construct and cannot be reduced to experiences in a single technological context as, e.g., information and communication technology. However, current methods to assess the broad construct of technology experience seem not appropriate anymore due to the fast technological developments. Nevertheless, mental models might be formed through prior experience with technology. Therefore, participants rated their general technology experience with several items (e.g., "If something breaks I usually seek to repair it by myself") (see [35] or [36]). Finally, items related to technology experience were summed into one weighted raw score, which was further converted into a percentage score. A maximum value of 100 indicates a high experience with technology.

Privacy Concept (PC). As we assumed that the general privacy attitude influences perceived privacy in technology-enhanced home environments, we asked participants to assess their privacy attitude in real-life and online contexts (e.g., "I am concerned about my privacy in everyday life.") [33,34]. Although Westin privacy segmentation [37], divided the population into three groups based on their level of privacy concern, we extracted two distinct clusters using hierarchical clustering: a group of participants with low concerns (1=*privacy unconcerned*) and a group with high concern in privacy (2=*privacy concerned*).

Dependent Variables

Knowledge about Technical Processes (KTP). We assessed the degree of congruence between the participants' mental models and the conceptual model of experts. Therefore, participants answered the question: "Explain…how data is transferred from the system to your physician?", which contained several aspects of computational processes (data transfer, connection, data storage and data access). Two independent raters coded each aspect regarding accuracy according to the coding scheme on a 7-point scale (0= *Participant did not pick up any aspect* to 6=*Best answer with complete set of information*). Both raters' rankings on each aspect were summed up to one raw score. Finally, the degree of accuracy was calculated as a percentage of the maximum raw score, which indicates a users' knowledge about technical processes similar to the conceptual model of experts. The median-split method was used to divide participants into two groups based on their KTP score. Participants with KTP scores below the median were categorized into a group of *low KTP* (1=1 thru 46), those with higher scores were classified into a group of *higher KTP* (2=47 thru 100).

Attitudes. Additional item clusters referred to subjective ratings of attitudes. The first assessed variable was **Privacy (P)**, which bundles privacy related topics, for example, perceived privacy in general (e.g., "The home monitoring system limits my privacy"), privacy as control over the system (e.g.," I would have to switch the system on and off at anytime") or worries about permanent surveillance (e.g., "I would not allow permanent surveillance by the system") A high privacy score indicates a high privacy concern. The concept of **Security (S)** is used as a combination of system security (e.g., "I think that the system is reliable" or "It is

likely that the transfer of my data is not sufficiently protected against unauthorized access by third parties") and personal health safety (e.g., "Permanent surveillance of vital parameters by the system would make me feel secure"). High scores on specific attitudes indicate high security concerns.

3.3.3. Reliability and Validity of Scales

To ensure a high quality of items within the pretest and posttest questionnaires, scale reliability and scale validity were analyzed. After excluding items which did not achieve the criteria of reliability and validity, Cronbach's Alpha values of scales reached .68 to .89. Compared to the acceptance level of .70 for empirical research [38], the majority of scale reliabilities were extraordinarily high and indicated internal consistence of scales. We are aware that the reliability score of .68 for *Privacy Concept* is questionable. However, we wanted to cluster participants into groups with similar privacy concept. According to Lienert & Raatz [39] a reliability value of <.60 is still acceptable to split participants into groups of same. Two

independent raters reached an inter-rater reliability of .88 for coding scheme *Knowledge about Technical Processes*.

Additionally, convergent and discriminant validity were examined using the principal component analysis with varimax rotation (Kaiser Normalization) to ensure that each item loaded on its particular anticipated scale. In total we extracted six factors, which explained 81.9% of variance. Focusing on our research question we will address four factors (*TE*, *PC*, *P* and *S*).

We used hierarchical clustering (average linkage between groups, see [19]) to classify subjects according to their privacy concepts in general. To select the best number of clusters we used the squared Euclidean distance of z-scores as an indicator. This enabled us to extract two distinct clusters: a group with low privacy concerns (*privacy unconcerned*) and a group with high privacy concerns (*privacy concerned*). The statements used to assess participants' *Technology Experiences* (*TE*), *Privacy Concepts* (*PC*) and attitudes such as *Privacy* (*P*) and *Security* (*S*) are shown in Table 1..

Table 1. Items of Technology Experience (TE), Privacy Concept (PC), Privacy (P) and Security (S)

Abbreviation	Item fulltext
TE5	I can assemble a prefabricated object (e.g., furniture) with construction manual by myself.
TE7	If something breaks I usually seek to repair it by myself.
PC1 (umcod)	Most businesses handle the personal information they collect about consumers in a proper and confidential way.
P3	I am concerned about my privacy in everyday life.
P5	I am likely to read the privacy policy.
P4	I must have the possibility to control which technical processes are running in the background, at any time.
P5	I must be in the position to control if data was collected by the system and if so which data.
P6	The system must provide me feedback which data was collected, stored and forwarded.
P7	I must be in the position to turn the system on and off at any time.
S4	It is likely that I cannot control, who has access to my health data.
S5	It is likely that my data transfer is not sufficiently protected from third parties.
S6	Permanent surveillance of vital parameters through the system would make me feel insecure.

3.3.4. Data Analysis

Twenty-four interviews were verbatim transcribed and analyzed using a previously developed coding scheme for *Knowledge about Technical Processes* (see section 3.3.2).

Q-Q plots and boxplots indicated scales (*TE* and *P*) and items (P5, P6, P7), which were not normally distributed. Therefore, we had to employ several statistical procedures. If the assumptions of parametric tests were met, data was analyzed by Pearson's product moment correlation and independent sample t test. For statistical analysis of non-parametric variables we used Spearman's rank correlation and Mann-Whitney U test. In addition, we will present results using mean value (*M*), standard deviation (*SD*) and median (*Mdn*). In general, when data analysis requires comparing different levels of measurements (parametric vs. non-parametric), we present data in a conservative fashion, e.g., by displaying results with median values.

Tests were met; data was analyzed by Pearson's product moment correlation and independent sample t test. For statistical analysis of non-parametric variables we used Spearman's rank correlation and Mann-Whitney U test. In addition, we will present results using mean value (*M*), standard deviation (*SD*) and median (*Mdn*). In general, when data analysis requires comparing different levels of measurements (parametric vs. non-parametric), we present data in a conservative fashion, e.g., by displaying results with median values.

The significance level of t tests, Mann-Whitney U test was set at $p<.05$. Outcomes of $p<.1$ are referred to as marginally significant. However, as we had a relatively small sample size (n=24), correlative associations might not be detected as significant. Therefore validity of assumptions will be guided by correlation coefficients. Only correlations greater than or equal to .3 and .5, which were referred to as moderate and strong effects [40], are reported.

4. Results

The results section is divided in four main parts:

1) sample description, 2) influence of user characteristics on *Knowledge about Technical Processes 3*) relation of user characteristics and perception of *Privacy* and *Security* and 4) association of *Knowledge about Technical Processes* on perception of *Privacy* and *Security*.

4.1. Participants

Participants, ranged in age from 19 to 76 years with a mean age of M=45.4 (SD=22.1) and came from a broad range of professions (e.g., medicine, economics and engineering). The first age group comprised 12 young adults aged between 19 and 34 years (M=24; SD=2.9). The second age group included 12 older adults aged between 48 and 76 years (M=66.8; SD=4.4). Both groups were gender-balanced with 50% men and 50% women. The majority of participants (n=20) was in good health conditions. Only four older female participants reported to have high blood pressure.

Corresponding to current literature (e.g., Heidrich et al., 2011) gender had a significant impact on STC scores (t(22)=2.2; $p<.05$). Male participants reported higher technical confidence (M=77.6; SD=10.4) than female participants (M=65.4; SD=15.8). In contrast, no gender differences could be found on scores of TE_{ICT} and $TE_{MedTech}$. However, t tests revealed significant age differences. Younger participants reported on both, technical self-confidence (M=79.7; SD=14) and experience with ICT (M=53.8; SD=8.1) higher scores than older participants (STC: M=63.4, SD=9.8 and TE_{ICT}: M=35.1; SD=11) (STC: t(22)=3.3; $p<.01$ and TE_{ICT}: t(22)=4.7; $p<.01$). Even though the overall experience with medical technologies was low, especially younger participants (M=4.1; SD=3.8) had significant lower experience with medical technologies in contrast to older participants (M=13.7; SD=10.5) (t(21)=-2.9; $p<.01$).

Assessing the *Privacy Concept* showed a positively skewed distribution. Therefore, we refrained from splitting by median, but rather used hierarchical clustering to split participants into two groups: (1) low privacy concern (n=16); and (2) high privacy concern (n=8).

All participants were German citizens and recruited through advertisements at public spaces, social networks and meeting places for older adults. Participants were novice users of technology-enhanced environments and not gratified for their efforts.

4.2. Influence of User Characteristics on Knowledge about Technical Processes

Participants were asked to describe how data is transferred to their physician. In correspondence with the results of the first study (see subsection 3.2), participants showed an average Knowledge about Technical Processes (KTP) (M=43.5; SD= 20.9) with a high variance within the sample. The aspects of data transfer, connection and data access showed the highest degree of congruence between mental models and the conceptual model.

Correlative analyses (Pearson was applied for interval-scaled and dichotomous data) were conducted for analyzing the influence of user characteristics on KTP (Table 2). In addition, t tests with KTP as depending variable were performed to verify the results of the dichotomous variable Privacy Concept (*privacy unconcerned vs. privacy concerned*). Correlations indicate that the knowledge about technical processes is moderately to strongly associated with age, TE and PC. Lower age (r=-.63; $p<.05$), high technical experience (r=.53; $p<.05$) and low concerns about privacy violations in general (r=-.42; $p<.05$) were moderately related to a higher score on KTP. T tests with privacy concept group as independent variable showed a significant difference on KTP scores. Privacy unconcerned participants showed higher KTP scores (M=49.6; SD=18) than privacy concerned participants (M=31.2; SD=21.9) (t(22)=2.2; $p<.05$).

4.3. Influence of User Characteristics on Privacy and Security Concerns

Results showed that the perception of privacy and security differed, which is displayed in Table 3. Scale values in general indicate that participants are most concerned about their *Privacy (P)* in technology-enhanced home environments (M=76.9; SD=17.8; Mdn=80.2). As Q-Q plots and boxplots indicated that the main scale of *Privacy* was non-parametric, median values will be presented in addition to means and standard deviations. Focusing on single privacy related items revealed that users regarded it as highly important that the system provides users with feedback, which data is collected, stored and forwarded (P6) (M=9.3; SD=1.6; Mdn=10.0). In contrast, security concerns were less pronounced (M=42.1; SD=29.8; Mdn=43.4). With regard to security aspects, the most prevalent concern was that participants cannot control, who has access to their health data (S4) (M=6.1; SD=3.4; Mdn=7.0). Privacy concern and security concerns showed no inter-scale correlation.

Pearson (used for interval-scaled and dichotomous data) and Spearman correlations (for ordinal-scaled data) were calculated for analyzing whether user characteristics are related with privacy and security concerns. While older participants reported privacy concerns with regard to technology-enhanced home environment than younger

participants (*r*=.46; *p*<.05), no correlations were found for security concerns. Technology experience showed no significant relation of with privacy and security concerns. As illustrated above, we expected a carry-over effect of general *Privacy Concept (PC)* to specific privacy concerns regarding technology-enhanced home environments. Surprisingly, *Privacy Concept* showed no significant correlation with Privacy. The results showed that the specific privacy concerns tested in the study are independent of perception of privacy in general. Independent sample *t* tests and Mann-Whitney *U* tests delivered the same results. *Privacy* (main scale and single items) in technology-enhanced home

environments did not differ between concerned and unconcerned participants. Nevertheless, *Privacy Concept* seemed moderately associated with *Security* (*r*=.46; *p*<.05). Privacy-concerned participants had higher security concerns than privacy-unconcerned participants.

Table 2. Bivariate correlations between user characteristics and Knowledge about technical processes (KTP).

	Age	Technology Experience	Privacy Concept
KTP	-.63**	.53**	-.42**

Note. **p<.05; *p<.1.

Table 3. Descriptive outcomes regarding general concerns and single items of Privacy (P) and Security (S).

Item	Statement	*M*	*SD*	*Mdn*
Privacy (scale in %)		76.9	17.8	80.2
P4	I must have the possibility to control which technical processes are running in the background, at any time.	7.5	2.7	8.0
P5	I must be in the position to control if data was collected by the system and if so which data.	8.8	2.1	10.0
P6	The system must provide me feedback which data was collected, stored and forwarded.	9.3	1.6	10.0
P7	I must be in the position to turn the system on and off at any time.	9.2	2.1	10.0
Security (scale in %)		42.1	29.8	43.4
S4	It is likely that I cannot control, who has access to my health data.	6.1	3.4	7.0
S5	It is likely that my data transfer is not sufficiently protected from third parties	5.3	3.4	5.5.
S6	Permanent surveillance of vital parameters through the system would make me feel insecure	4.1	3.0	3.0

Note. Scale values indicate degree of concerns (100=highest concern) and item values the level of agreement with different privacy and security statements (1=*very low agreement* to 10= *very high agreement).*

4.4. Influence of Knowledge about Technical Processes on Privacy and Security Concerns

In order to analyze whether technical knowledge about technology-enhanced home environments is associated with privacy and security concerns, two-tailed *t* tests and Mann-Whitney *U* tests were run with *high vs. low KTPs* as independent variables. Pearson and Spearman correlations were calculated to verify the results.

The overall scales of Privacy and Security did not significantly differ depending on the degree of congruence between mental models and the conceptual model. Correlating knowledge about technical processes with attitudes such as privacy and security confirmed this result. Knowledge about Technical Processes did not show any correlative association with attitudes such as privacy and security.

5. Discussion

This article aimed at getting a better understanding about the technical knowledge of end users regarding technology-enhanced home environments and individual user factors, as knowledge structures play an important role for the perception of privacy and security concerns. In the following sections we discuss the findings and implications of both studies.

5.1. The Role of User Factors on Knowledge about Technical Processes

We start this section by discussing mental models represented as knowledge about technical processes in a general way. In a second step, we examine existing associations between different user factors and technical knowledge.

In order to get a detailed understanding about the technical processes taking place in technology-enhanced home environments, we interviewed different experts, who were involved in the development of the *Future Care Lab*. We used experts' answers to construct a generic conceptual model of the technology-enhanced home environment technology. We compared the responses of participants on technology-related questions with the conceptual model of experts to assess the degree of technical knowledge on different levels.

Our observations confirm Norman's [12] argumentation, who characterized mental models as among other things *incomplete*. The results of the first study showed a clear lack of knowledge about the underlying technical processes of technology-enhanced home environments. This was especially the case for questions regarding the transmission of data between different medical devices (blood pressure monitor, scale etc.) and the system. For instance, despite the fact that a data transmission cable was visibly connected to the blood pressure meter, one participant answered that "*data is transferred via rays similar to a remote control of a television*" ($N_{1.12}$). The majority of participants misinterpreted the wire as a power cable instead of the data transfer cable that it really was. It appears that the participants' mental models of new technologies assume that data transfer nowadays always works wirelessly. Therefore, preexisting mental models might have contributed to ruling out the option of a wired data transfer. The question of how data is transferred to a remote physician (Q3) revealed the highest degree of congruence between the participants' mental models and the generic conceptual model. However, the results of both studies show that the level of knowledge about technical processes is generally quite low.

When looking at individual user factors in the second study, it became evident that knowledge about technical processes differs between user groups. Results support the hypothesis that knowledge about technical processes differs depending on age [13] and technology experience [12]. Regardless of gender, younger in terms of technology more experienced participants showed more accurate knowledge about technical processes.

The results also showed that participants' degree of technical knowledge is linked with the privacy concept in daily life as well as online. Participants who showed a higher degree of knowledge were less concerned about their privacy than participants with less knowledge. This could be explained by Spiekermann [41] who concluded that "privacy has actually for decades been defined in terms of control" (p. 2). Therefore, it might be possible that higher technical knowledge contributed to the perception of increased control over a system. So due to their higher technical knowledge these participants still feel like being in control of their own privacy. Thus they were less concerned about their privacy compared to those participants with less knowledge, who felt like they were not in control.

5.2. Perception of Privacy and Security

The analysis of privacy and security concerns revealed a comprehensive image of users' attitudes towards technology-enhanced home environments. Overall, participants were most concerned about their privacy. Above all, users pointed out the importance of feedback through the system i.e. which data is collected, stored and forwarded. While it is expectable that feedback helps to establish positive attitudes about technology-enhanced home environments, it is noteworthy that privacy concerns

increase with age. Especially older adults benefit from the functionalities, which technology-enhanced home environments offer. The results gained in our study clearly show that everyone, and in particular older adults, expressed the desire to control the system and maintain a feeling of privacy and security. Moreover, we could not confirm our exploratory impression of a carry-over effect of general privacy concerns to privacy concerns regarding technology-enhanced home environments.
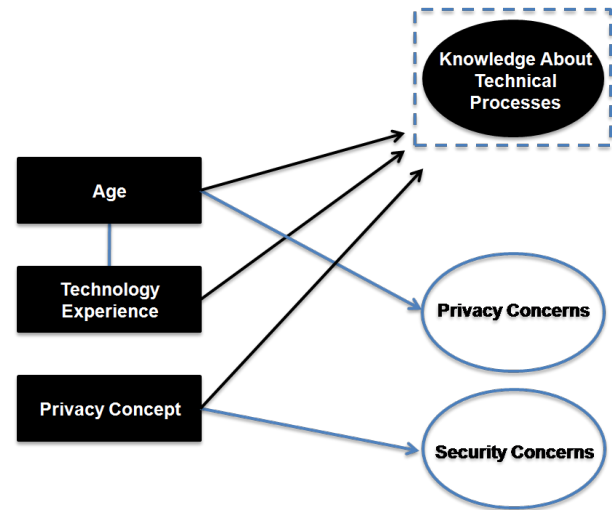
Figure 6. Schematic conclusion of the main findings.

Influences of user characteristics on knowledge about technical processes (black colored).

5.3. Association of Knowledge about Technical Processes with Privacy and Security

We also tried to answer the question, how technical knowledge is influencing attitudes such as privacy and security Therefore, we associated the responses to Q3 ("Explain…how data is transferred from the system to your physician.") with the scales of privacy and security.

Neither perceived privacy concerns, nor security concerns differed depending on the technical knowledge. The results were contrary to our expectations and work of other authors (e.g., [18,19,22]) and therefore confusing. Somehow, more appropriate mental models (represented as a higher degree of congruence between the participants' knowledge about technical processes in technology-enhanced home environments and the conceptual model) did not seem to influence the perception of privacy and security in such systems, but only privacy in general.

The fact that knowledge about technical processes is not related with attitudes such as privacy and security in technology-enhanced home environments leaves room for interpretation. Acquisti and Grossklags [19] directly investigated the degree of knowledge about "privacy risks and modes of protection" (p.29) and how much participants care. Here the "lack of knowledge about technological […] privacy protection" (p.29) became obvious. In contrast, our second study did not directly address privacy protection.

Instead, the study assessed general computational processes of knowledge (see Q3), which might explain why we could not detect relations between attitudes such as privacy and security and knowledge.

Summing up the results, we can conclude that general structural knowledge about technical processes of technology-enhanced home environments is not related to attitudes such as privacy and security in such technology-enhanced environments.

5.4. Limitations and Future Research Questions

Both studies helped to gain first insights into the relations among users' factors, mental models, privacy, security, trust and conventional acceptance factors in the context of technology-enhanced home environments. However, not all research questions could be answered with the results gained in the studies and further research questions arose during the analysis of the data. In addition, the following limitations need to addressed in further research.

(1) As mentioned in section 5.3, one limitation refers to the methodology used to assess knowledge. Due to the vague content of Q3, it is difficult to describe how knowledge about privacy risks, security risks and protection mechanism as well as unwanted access possibilities influence the perception of privacy and security in technology-enhanced home environments. Instead of assessing knowledge on a general, structural level, concrete knowledge about privacy risks and protection (e.g., according to [19]) should be assessed. Here it might help to modify the content of each question (e.g., "How can you avoid unauthorized data access?"). In addition, we should think of using a knowledge test (e.g., "I can permanently delete my personal data from the web so no third person can ever retrieve my data" or "It is possible that my children have remote access to my data, while at the same time the access is completely denied for unwanted third persons.").[1]

(2) A further remark relates to the pretest and posttest questionnaires design. Several questionnaire scales, e.g., privacy scale and technology experience scale, should be improved. Due to reliability and factor analysis (see section 3.3.3) most scales contained only a small number of items. Retrospectively, a restriction regarding the content of the privacy scale was found. As mentioned earlier, we described privacy as control over the system, which represents a commonly used understanding of privacy [41]. Hence, the items of the posttest questionnaire intended to assess perceived privacy in general, privacy as control over the system and concerns about permanent surveillance. However, it appeared that Privacy embedded only control related items and excluded sensitive concerns regarding privacy (e.g., "I am concerned about my privacy" or "Due to the home-monitoring system I would behave differently"). An

improved version of the questionnaires should include more items.

For further studies a direct comparison of items ("I am concerned about privacy in general" vs. "I am concerned about my privacy in technology-enhanced home environments") might be helpful.

(3) Moreover, we have to limit our results to the German culture and values. Other cultures may show different relations to technology and therefore perceive technology differently, e.g., Asian cultures [42]. Therefore, it is necessary to consider "cultural views on technology acceptance" ([43], p.1). Further, the tested sample of older adults was quite homogenous with respect to good health conditions and active lifestyles. We assume that different health conditions might influence the perception of technology-enhanced home technologies [44]. Additionally, we did not differentiate between users with varying technological backgrounds in detail. Here, we might compare user groups, who are dealing with information technology on an amateur level and participants, who deal with technology due to their profession. Results could emphasize the influence of knowledge about technical processes on different attitudes.

(4) Finally, we only tested a limited number of participants. Therefore results provide only tendencies of insights about mental models and their relations to privacy and security. Future studies need to test a larger sample.

The subject of knowledge structures and influencing factors on the perception of privacy and security is very complex. This contribution could only cover a small part of interesting relations and hopefully pave the way for further research in this exciting and relevant field of technology-enhanced environments.

---

[1] We consider that both statements require higher knowledge about information technology. The next diagnostic test should be developed to cover a broader range of participants' knowledge.

REFERENCES

[1] OECD (2005). Factbook 2005 economic, environmental and social statistics. Paris: OECD Publishing.

[2] Wilkowska, W., & Ziefle, M. (2011a). Perception of privacy and security for acceptance of E-health technologies: Exploratory analysis for diverse user groups. In Proceedings of the 5th International IEE conference on Pervasive Computing Technologies for Healthcare. 593-600.

[3] Zur Hausen, H. (Ed.) (2009). Gained years. Recommendations of the 'academic group aging' in Germany (Gewonnene Jahre. Empfehlungen der Akademiengruppe Altern in Deutschland). Nova Acta Leopoldina, 107 (371). 1-92.

[4] Weiner, M., Callahan, C.M., Tierney, W. M., Overhage, M., Mamlin, B., & Dexter, A. (2003). Using information technology to improve the health care of older adults. Annals of Internal Medicine, 139, 430-436.

[5] Ziefle, M., Röcker, C.,Wilkowska, W., Kasugai, K., Klack, L, Möllering, C., & Beul, S. (2011). A multi-disciplinary approach to ambient assisted living. In C. Röcker, & M. Ziefle, (Eds.). E-Health, Assistive Technologies and Applications for Assisted Living: Challenges and Solutions (pp. 76-93). Hershey, P.A.: IGI Global.

[6] Kleinberger, T., Becker, M., Ras, E., Holzinger, A., & Müller, P. (2007). Ambient intelligence in assisted living: Enable elderly people to handle future interfaces. In C. Stephanidis (Ed.). LNCS: Vol. 4555. Universal Access in Human-Computer Interaction: Ambient Interaction (pp. 103-112). Berlin, Heidelberg, New York: Springer.

[7] Caine, K. E., Zimmerman, C. Y., Schall-Zimmerman, Z., Hazlewood, W. R., Sulgrove, A.C., Camp, L. J., Connelly, K. H., Huber, L. L., Shankar, K. (2010). DigiSwitch: design and evaluation of a device for older adults to preserve privacy while monitoring health at home. In Proceedings of the ACM SIG on International Health Informatics (IHI'10) (pp. 153-162). Washington: ACM.

[8] Nixon, P., Wagealla, W., English, C., & Terzis, S. (2004). Security, privacy and trust issues, In D. Cook & S. Das (Eds.). Smart Environments: Technology, Protocols and Applications. (pp. 220-240). London, UK: Wiley.

[9] Weiser, M., Gold, R., & Brown, J. S. (1999). The origin of ubiquitous computing research at PARC in the late 1980s. IBM System Journal, 38, 693-696.

[10] Johnson, J., & Henderson, A. (2011). Conceptual models: Core to good design. San Rafael, California: Morgan & Claypool Publishers.

[11] Gage, N.L., & Berliner, D.C. (1979). Educational psychology (Pädagogische Psychologie). München: Urban & Schwarzenberg.

[12] Norman, D. A. (1983). Some observations on mental models. In D. Gentner, & A. A. Stevens (Eds.), Mental Models (pp. 7-14), Hillsdale, New Jersey: Erlbaum.

[13] Calero-Valdez, A.; Ziefle, M. Alagöz, F., & Holzinger, A.(2010). Mental models of menu structures in diabetes assistants. In K. Miesenberger et al. (Eds.), LNCS: Vol. 6180. 12th ICCHP- International Conference on Computers helping people with special needs. Part II (pp. 584-591). Berlin, Heidelberg: Springer.

[14] Wilkowska, W., & Ziefle, M. (2011b). User diversity as a challenge for the integration of medical technology into future home environments. In M. Ziefle, & C. Röcker (Eds.). Human-Centred Design of eHealth Technologies. Concepts, Methods and Applications (pp. 95-126). Hershey, P.A.: IGI Global.

[15] Ziefle, M., Röcker, C., & Holzinger A. (2011). Medical technology in smart homes: Exploring the user's perspective on privacy, intimacy and trust. In Proceedings of the 35th Annual IEEE Computer Software and Applications Conference. 410-415.

[16] Himmel, S. (2011). Acceptance of home-integrated information- and communication technologies - when your living space knows what you do. Paper presented at the 7th Conference of the Austrian Computer Society Workgroup: Human-Computer Interaction (USAB 2011): Information Quality in Healthcare. Graz, Austria.

[17] National Consumer Health Privacy Survey (2005, November). Retrieved December 30, 2012, from http://www.chcf.org/~/media/MEDIA%20LIBRARY%20Fil es/PDF/C/PDF%20ConsumerPrivacy2005ExecSum.pdf

[18] Kaasinen, E. (2003). User needs for location-aware mobile service. Personal and Ubiquitous Computing, 7, 70-79.

[19] Acquisti, A., & Grossklang, J. (2005). Privacy and rationality in individual decision making, IEEE Security & Privacy 2005 (pp. 24-30). New York: IEEE Computer Science.

[20] Wash, R. (2010). Folk models of home computer security. In Proceedings of the 6th Symposium on Usable Privacy and Security. 1-16.

[21] Wash, R., & Rader, E. (2011). Influencing mental models of security: A research agenda. In Proceedings of the New Security Paradigms Workshop (NSPW) (pp. 57-66). Marshall, CA: ACM.

[22] Asgharpour, F., Liu, D., & Camp, L. J. (2007). Mental models of security risks. In S. Dietrich & R. Dhamija (Eds.), LNCS: Vol. 4886. Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security (pp.367-377). Heidelberg: Springer.

[23] Woolham, J., & Frisby, B., (2002). Building a local infrastructure that supports the use of assistive technology in the care of people with dementia. Research Policy and Planning, 20, 11-24.

[24] Röcker, C., Wilkowska, W., Ziefle, M., Kasugai, K., Klack, L., Möllering, C., & Beul, S. (2010). Towards adaptive interfaces for supporting elderly users in technology-enhanced home environments. In: Proceedings of the 18th Biennial Conference of the International Communications Society: Culture, Communication and the Cutting Edge of Technology. June 27 - 30, Tokyo, Japan. CD-ROM.

[25] Ziefle, M., Röcker, C., Kasugai, K., Klack, L., Jakobs, E.-M., Schmitz-Rode, T., Russell, P., & Borchers, J. (2009). eHealth – Enhancing mobility with aging. In M. Tscheligi, B. de Ruyter, J. Soldatos, A. Meschtscherjakov, C. Buiza, W. Reitberger, N. Streitz, & T. Mirlacher (Eds.), Roots for the Future of Ambient Intelligence, Adjunct Proceedings of the Third European Conference on Ambient Intelligence (AmI'09). 25-28.

[26] Klack, L., Schmitz-Rode, T., Wilkowska, W. Kasugai, K., Heidrich, F., & Ziefle, M. (2011). Integrated home monitoring and compliance optimization for patients with mechanical circulatory support devices (MCSDs). Annals of Biomedical Engineering, 39, 2911-2921.

[27] Klack, L., Kasugai, K., Schmitz-Rode, T., Röcker, C., Ziefle, M., Möllering, C., Jakobs, E.-M., Russell, P., & Borchers, J. (2010). A personal assistance system for older users with chronic heart diseases. In Proceedings of the Third Ambient Assisted Living Conference (AAL'10), January 26 - 27, VDE

Verlag, Berlin, Germany, CD-ROM.

[28] Heidrich, F., Ziefle, M., Röcker, C., & Borchers, J. (2011). Interacting with smart walls: A multi-dimensional analysis of input technologies for augmented environments. In Proceedings of the ACM Augmented Human Conference (AH'11) (pp. 1-8), New York: ACM.

[29] Van der Veer, G. C., & Puerta Melguizo, M. C. (2003). Mental models. In J.A. Jacko, & A. Sears (Eds.) The Human-Computer Interaction Handbook: Fundamentals, evolving Technologies and emerging applications (pp. 52-80). New Yersey: Lawrence Erlbaum Associates.

[30] Sasse, M. A. (1997). Eliciting and describing users' models of computer systems. (Unpublished doctoral dissertation). School of Computer Science, The University of Birmingham, Birmingham.

[31] Van der Veer, G. C., Kok, E., & Bajo, T. (1999). Conceptualising mental representations of mechanics: A method to investigate representational change. In D. Kayser, & S. Vosniadou (Eds.), Modelling changes in understanding: Case studies in physical reasoning. Elmsford, NY: Pergamon.

[32] Beier, G. (1999). Locus of control when interacting with technology (Kontrollüberzeugungen im Umgang mit Technik). Report Psychologie, 24, 684-693.

[33] Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of internet users: Self-reports versus observed behavior. International Journal of Human-Computer Studies. 203-227.

[34] Taylor, H. (2003, March 19). Most people are "privacy pragmatists" who, while concerned about privacy, will sometimes trade it off for other benefits. Retrieved December 30, 2012, from http://www.harrisinteractive.com /vault/Harris-Interactive-Poll-Research-Most-People-Are-Privacy-Pragmatists-Who-While-Conc-2003-03.pdf

[35] Gaul, S., & Ziefle, M. (2009). Smart home technologies: Insights into generation-specific acceptance motives. In A. Holzinger & K. Miesenberger (Eds.), LNCS: Vol. 5889. USAB 2009 (pp. 312-332). Berlin, Heidelberg: Springer.

[36] Ziefle, M., & Schaar, A. K. (2010). Technical expertise and its influence on the acceptance of future medical technologies.

What is influencing what to which extent? In G. Leitner, M. Hitz, & A. Holzinger (Eds). LNCS: Vol. 6389. HCI in Work & Learning, Life & Leisure (pp. 82-100). Berlin, Heidelberg: Springer.

[37] Westin, A. (1999). Freebies and privacy: What the net users think. Retrieved February 22, 2013, from http://www.content.imamu.edu.sa/scholars/it/net/westin.pdf

[38] Arning, K., & Ziefle, M. (2007). Understanding differences in PDA acceptance and performance. Computers in Human Behaviour, 23. 2904-2927.

[39] Lienert, G., & Raatz, A. (2001). Test analysis and test development (Testanalyse und Testkonstruktion). Weinheim: Beltz.

[40] Sedlmeier, P., & Renkewitz, F. (2008). Research methods and statistics in psychology (Forschungsmethoden und Statistik in der Psychologie). München. Pearson Studium.

[41] Spiekermann, S. (2005, July). Perceived control: Scales for privacy in ubiquitous computing. 10th International Conference on User Modeling. Retrieved December 1, 2012, from http://dx.doi.org/10.2139/ssrn.761109

[42] Shin, D. H. (2010). Ubiquitous computing acceptance model: End user concern about security, privacy and risk. International Journal of Mobile Communications, 8, 169-186.

[43] Alagöz, F., Ziefle, M., Wilkowska, W., & Calero Valdez, A. (2011). Openness to accept medical technology – a cultural view. In H. Holzinger & K.-M. Simonic (Eds.), LNCS: Vol. 7058. Human-Computer Interaction: Information Quality in eHealth. (pp. 151-170). Berlin, Heidelberg: Springer.

[44] Ziefle, M. (2012). Uncertainties that come with the introduction of new technologies. Usage barriers using the example of medical technologies within home environments (Ungewissheit und Unsicherheit bei der Einführung neuer Technologien. Nutzungsbarrieren am Beispiel von Medizintechnologien im häuslichen Umfeld). In S. Jeschke, E.-M. Jakobs, & A. Dröge (Eds.), Uncertainties that come with the introduction of new technologies (Ungewissheit und Unsicherheit bei der Einführung neuer Technologien) (pp. 83-104). Berlin: Springer Gabler.