‘Home, Smart Home’ – Exploring End Users’ Mental Models of Smart Homes

Verena Zimmermann, Merve Bennighof, Miriam Edel, Oliver Hofmann, Judith Jung, Melina von Wick

FAI - Work and Engineering Psychology - Technische Universität Darmstadt, Germany

zimmermann@psychologie.tu-darmstadt.de, m.bennighof@web.de, miriam.edel@t-online.de, oli.hofmann@gmx.net, judith.jung@online.de, melina.vonwick@gmail.com

Abstract

Smart Home technologies are increasingly available for private households. Still, the level of acceptance varies among potential users. Possible reasons include a lack of knowledge and negative user perceptions, e.g. in terms of privacy and security. To support researchers and practitioners in designing Smart Home technologies that align with the users’ needs and expectations the mental models of 42 potential Smart Home users were examined using a semi-structured interview approach. The results revealed that the users’ understanding of Smart Homes was rather superficial. The use cases and benefits reflected the options currently available for sale, such as automated heating and lighting. Nearly all users doubted that their data was secure within a Smart Home. However, the scenarios described often included remote control of the Smart Home and thus a transfer of the data to the internet. Hence, future work could explore options to increase Smart Home security by e.g. limiting internet access to certain user-defined scenarios.

1 Introduction

In today’s world there is a demand for innovative security technologies to protect sensitive data when using an increasing number of digital and inter-connected products and services. An important example is provided by Smart Home technologies that are already, and increasingly will be, present in our current and future homes. As Smart Home technologies are highly interwoven with our private life, issues such as trust, usability, controllability and security are essential.

According to Balta-Ozkan et al., (2013, p.364) the term Smart Home is defined as “a residence equipped with a high-tech network, linking sensors and domestic devices, appliances, and features that can be remotely monitored, accessed or controlled, and provide services that respond

Veröffentlicht durch die Gesellschaft für Informatik e. V. 2018 in
R. Dachselt, G. Weber (Hrsg.):
Mensch und Computer 2018 – Workshopband, 02.–05. September 2018, Dresden.
 https://doi.org/10.18420/muc2018-ws08-0539

to the needs of its inhabitants". As such, Smart Homes provide a huge potential: they can increase domestic comfort, security and energy efficiency, as well as support for senior citizens, e.g., by monitoring their health status (Demiris et al., 2004).

Over the last years, the spread of Smart Home technologies has increased, but not yet overcome the threshold of the mass market (GfK, 2016; Schulze-Sturm, 2016). Often companies face problems like low acceptance rates due to insufficiently addressing end users (Ogonowski et al., 2016).

1.1 Mental Models

To capture the understanding of end users, psychological research often uses the concept of mental models (Kang et al., 2015), which represent the structure and functioning of a system, help the user to understand the system and to draw conclusions (Borgman, 1986). Among others, mental models can be captured by interviews (e.g. Wash, 2010), card-sorting (e.g. Shirehjini et al., 2016), sketching, or Think-Aloud techniques (e.g. Kang et al., 2015).

Even though usually simplified and unstable (Norman, 1983), mental models offer valuable information concerning user requirements and expectations and can be used to improve user interfaces. Stewart and Lacey (2011) also call for the application of mental model approaches in the security and privacy area to increase the effectiveness of awareness methods by placing the focus on the targeted audience. Therefore, this study uses mental models to explore current user perceptions, expectations and concerns regarding Smart Homes.

1.2 Mental Models and User Perceptions of Smart Homes

Previous research on mental models of Smart Homes showed that end users often think of an increase in comfort and security, the management of energy use and housekeeping activities (Wilson et al., 2017). According to Schulze-Sturm (2016), there is a large interest in Smart Home technologies, but the level of acceptance varies among potential end users. Influencing factors identified by Green et al. (2004) are for example usability, cost, the system's flexibility, trustworthiness and data security. Market research identified cost, lack of awareness and privacy concerns as main barriers for adoption (GfK, 2016). In addition, Emami-Naeini et al. (2017) found that with the rapid growth of the Internet of Things (IoT) the demand for transparency, control and instruments that ensure the privacy and data security of users increases.

In terms of privacy and security, users generally felt uncomfortable about storing private and sensitive data like bank data or periods of absence within IoT-devices (Emami-Naeini et al., 2017). However, Zeng et al. (2017) found that end users' concerns regarding Smart Homes concentrated more on physical security than on privacy. A potential reason might be that most end users cannot fully determine the privacy risks of Smart Homes due to a lack of technical understanding, as users with more sophisticated mental models of Smart Homes also had more detailed concepts of potential threats.

Still, it is not finally clear in what way Smart Homes need to be designed to align with users' needs and perceptions. This study thus examines the mental models of potential and actual

Smart Home users and analyzes user perceptions in terms of privacy and security. Furthermore, implications of the results for Smart Home researchers and developers will be discussed in the context of other results from the literature. These findings should be addressed in addition to legal and other requirements that are not subject of this paper.

By interviewing a relatively large sample of more than 40 users and comparing non-experienced and experienced users this study adds to the growing body of literature on Smart Homes users’ mental models. The research was guided by the following question that was further divided into four sub-questions: What are the end users’ mental models of Smart Homes?

1. What is the end users’ understanding of the term “Smart Home”?

2. Which benefits do end users ascribe to Smart Homes?

3. What do end users think how Smart Homes function?

4. Which security and privacy perceptions do end users have of Smart Homes?

2 Method

The following section describes the study sample and procedure as well as the structure and contents of the semi-structured interview.

2.1 Sample

The sample consisted of N = 42 participants ranging from 20 to 57 years (M = 33.69, SD = 13.41). A total of 24 (57%) participants were male. On a seven-point scale the mean experience with IT-Security was rated as M = 3.10 (SD = 2.09). According to our definition described in section 2.2. half of the participants were classified as experienced, the other 21 were rated as non-experienced. The participants covered a large variety of occupations including six people with an IT background and nine people with an engineering or technical background. A majority of 23 participants attained a graduate degree, followed by nine participants with a completed vocational training. The participants were recruited via mailing lists and snowball-sampling in several cities in Germany. They were compensated for their participation with 5€-Amazon vouchers.

2.2 Study Design and Procedure

A semi-structured interview was used to investigate mental models, user perceptions, and user requirements of Smart Homes (see Appendix). Using a two-step process, participants were allocated to one of four groups.

In a first step, participants were classified as experienced or non-experienced as previous research showed that more experienced end users also have more accurate and detailed mental models (Staggers & Norcio, 1993). They were classified as experienced when having used or

currently using central Smart Home controls in their own home and/or using a minimum of three automated rule-based technologies (e.g. timer, motion sensor).

In a second step, participants were randomly allocated to one of two methods to capture mental models, a) a verbal explanation or b) drawing a sketch of their understanding of a Smart Home.

At the beginning of the interview, participants were given a brief overview about the study and its aims, followed by questions about their Smart Home knowledge, general perception and expected benefits of Smart Homes. Apart from open questions the participants were asked to list associations with the term "Smart Home" in written form. For classification, they were then asked about their past and present usage experiences of Smart Home technologies. Next, the participants were randomly allocated to either verbally explaining or drawing a sketch of Smart Home functions, components and their interactions. The sketching method was combined with the Think-Aloud technique in which participants were asked to verbally explain their sketches. The combination of drawing and verbally explaining was also found to be effective by Zeng et al. (2017). In a last step, participants were asked about concerns and risks concerning Smart Home use, focusing on security, privacy and possible threats.

After the semi-structured interview, participants were asked to provide demographics and to fill out the Internet User's Information Privacy Concerns (IUIPC) questionnaire in the translated (English-German) version (Malhotra et al., 2004). It assesses information on privacy concerns with six items on a seven-point scale. It can be divided into three subscales (1) Collection, (2) Control and (3) Awareness of Privacy Practices.

2.3 Data analysis

The semi-structured interviews and the list of associations with the term "Smart Home" were transcribed and analyzed separately with an open coding approach according to Mayring (2002) using the MAXQDA Version 12 (Verbi, 2015). The categories and subcategories were formed and discussed in two rounds of analysis. For transcriptions, informal language was kept, however reduced by redundant words. Each transcript was independently analyzed by two raters. The correlation of the number of notions in each category was $r = .90$.

3 Results

For the analysis the absolute number of notions within a category or subcategory was counted and is represented by the numbers in brackets. As participants were able to list several aspects that fall within one category, the number is not always equal to the number of participants.

A descriptive analysis revealed only minor differences for the frequency of terms mentioned in the analyzed categories between non-experienced (N = 21) and more experienced (N = 21) participants. For example, more experienced users named more aspects when *defining the term Smart Home* (90) and describing the *interaction between Smart Home components* (51) compared to non-experienced users (67 and 27). However, non-experienced users slightly more often raised *concerns resulting from Smart Home use* (71) than more experienced users (61).

In terms of *Smart Home functions*, *perceived benefits*, *Smart Home components*, the assessment of *privacy-sensitive Smart Home data*, *potential attack scenarios* and *perceived data security* the number of notions did not vary considerably. The following results are thus presented for the complete sample regardless of the level of Smart Home experience.

Understanding of the term Smart Home. Participants defined Smart Homes as a control mechanism of domestic appliances (28) such as light, fridge or washing machine that could be accessed via various media (28) such as smart phone or tablet. The definition often included remote control (23) and networking (22) of all devices and components. The participants mainly mentioned heating (23), lighting (29), domestic appliances (27), and roller shutters (12) as examples of Smart Home appliances. These results from the interviews were reflected by the separately coded list of terms associated with Smart Homes. A summary of the most frequently named associations is provided in Table 1. Participants associated positive expectations and advantages (45) with Smart Homes but also mentioned concerns (43) like security concerns (8) or potential technical failure (6).

Categories	**Examples**	**Percent**
Smart Home Components	(145 notions)	(34%)
End Devices	lighting, heating, shutters, fridge, apps, smart phone	49%
Central Hub/ Control	Amazon Alexa, Google Home, Siri, Xbox	32%
Smart Home Use Cases	(97 notions)	(23%)
Comfort	facilitation of everyday life, remote control	75%
Security	video observation, safety management, protection	24%
Benefits	(45 notions)	(11%)
Advanced Technology	automation, progress, artificial intelligence, digital	22%
Positive Feelings	to be comfortable, flexible, cozy	20%
Concerns	(43 notions)	(10%)
Privacy/Security Concerns	data security, security flaw, advertisement	53%
Technical Concerns	break down, error-proneness, outage	33%

Table 1: Overview of the most frequently mentioned associations with the term Smart Home

Smart Home Benefits. As advantages of Smart Homes the participants mentioned the facilitation of everyday life and comfort (38), energy efficiency (17), and security (13). For example one participant described the facilitation aspect as follows: “[…] when you go on vacation und you think ‘Ah, I forgot to switch off the lights!’ and then you can switch off the lights via mobile phone.” Furthermore, participants often mentioned various benefits like comfort or security in their lists of associations (see Table 1). For example, they listed remote control of temperature regulation as comfort and video observation as security aspects.

Functioning of Smart Homes. Most participants were aware that Smart Homes consist of some kind of control device (40), end devices (39) like lighting or roller shutters, and a coordinating central hub (25). Participants mainly believed that the devices were connected via Wi-Fi (31), radio (15), or cable (13). These components were mentioned regardless of whether the participants drew a sketch (N = 21) or verbally described how Smart Homes worked according to

their understanding (N = 21). Further details or technical components were only rarely mentioned, e.g. sensors (12), servers (7) or software (5). Examples for the sketches created by the participants are depicted in Figure 1. While some made use of a graphical representation of a home (left picture), others used a more abstract level to visualize processes or interactions (right picture).

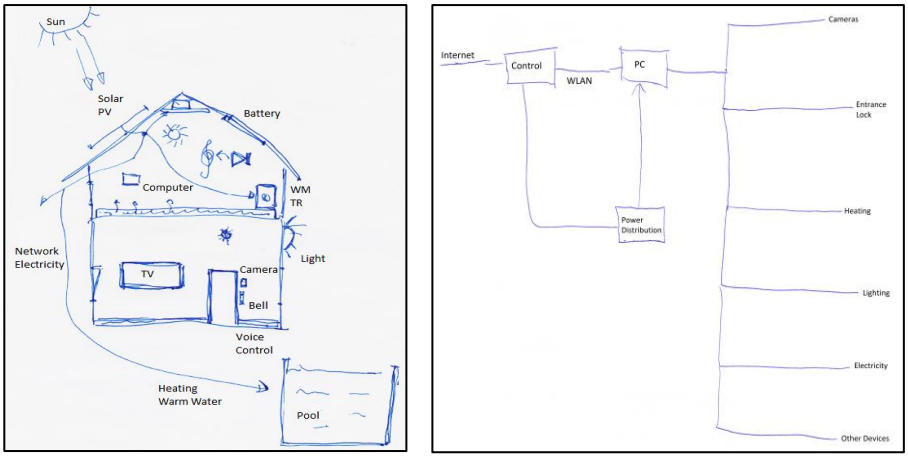


Figure 1: Exemplary sketches to visualize the functioning of a Smart Home (Captions were translated)

Privacy and Security Perceptions. Overall, 39 out of 42 participants were not convinced that their data was secure within a Smart Home. Especially sensitive data such as bank details (14), times of absence (10), and personal preferences (9) were most frequently regarded as critical in terms of privacy. Participants often feared hacker attacks (27) and data abuse (18) by burglars or the Smart Home provider. One participant noted "when something goes wrong, a stranger simply could get into the apartment without having to really break in, because then, the door opens on its own." Another participant questioned, "in what way they (the providers) could sell the data or, accordingly, collect it." Apart from that, technical deficiencies (22) and the perceived dependence (8) from the technology were viewed as problematic. The participants' general privacy concerns measured with the IUIPC were rated with M = 4.26 (SD = 1.23) out of seven points.

4 Discussion and Conclusion

The aim of this study was to explore the end users' perceptions, expectations and concerns regarding Smart Homes. Therefore, 42 participants with varying degrees of Smart Home experience were interviewed using sketches or verbal descriptions to capture their mental models. In contrast to the results of Staggers and Norcio (1993) only minor differences were identified between participants with and without Smart Home experience according to our definition. An explanation might be offered by the "soft" definition of Smart Home experience and users' little overall experience.

The term “Smart Home” was mostly associated with automated and connected domestic appliances such as lighting and heating. Many participants also expressed the idea of controlling these appliances remotely and with different devices such as smart phones. In line with the results of Wilson et al. (2017), participants named the facilitation of everyday life, higher comfort and security levels and an increase in time and energy efficiency as potential benefits. Potential users’ mental models of Smart Homes consisted of control devices, a central hub and end devices interconnected via Wi-Fi, radio, or cable. To that end, the users’ understanding of the functioning of Smart Home technologies was in line with the technical reality, but somewhat simplified. In most cases no technical details about the storage and processing of data or the programming used to execute the functionality, e.g. unlocking a door upon arrival, were mentioned. In terms of security and privacy, nearly all participants felt that their data was not secure in a Smart Home. Most concerns expressed centred around burglary, hacker attacks, data theft, and data abuse. Especially the collection and storage of sensitive data like bank details, preferences or times of absence was perceived as critical.

Limitations. The sample mainly consisted of people with little IT Security expertise and Smart Home experience. Thus, the results might not be representative for the entirety of prospective Smart Home users. Experience was measured by the number of automated appliances and/or the possession of a central Smart Home hub. However, few participants owned a central hub or interconnected appliances. This displays the current state that about 15% of German households (Statista, 2018) use Smart Home technologies with a varying degree of automation. Still, future studies would benefit from participants with more Smart Home experience to explore differences between people with and without actual experience.

Mental Models of Smart Homes. Mental models seemed to be affected by the technologies advertised in the media and more widely available by now. For example, many people named the automation of lighting and heating as Smart Home functions for which sensors and light bulbs are readily available in hardware stores and apps available for the smart phone. Among the most commonly described scenarios were those of arriving at home and having appliances working by the time of arrival (e.g. heating and lighting on) and of using devices to increase home security (e.g. detection of break-ins) while being away. In contrast to that, other scenarios were rarely mentioned, e.g. the potential use of Smart Homes for health care and supporting elderly people. Possible explanations include the demographics of our sample and the rare presentation of this use case in the public media.

In this regard, our results reflect those provided by Jakobi et al. (2017). The Smart Home users in their long-term field study often came up with what smart homes already offered when asked what could be improved or automated. The authors suggest providing more orientation towards possible practices, routines and use cases to facilitate choice of suitable Smart Home technologies. In line with that, Smart Home researchers and practitioners should consider that people seem to expect functions they can easily recall or are familiar with. Research from other fields already showed that preferences are not only influenced by novelty but also familiarity (e.g. Hekkert et al., 2003). Further effects such as the availability heuristic, the tendency to rate easily recallable aspects as more important, might also play a role. Possible implications for Smart Home developers might be to familiarize potential users with new technological features or use cases beforehand and to provide easily accessible orientation. Another option might be to combine new technologies with familiar or already available technologies.

Technical Deficiencies. About half of the participants anticipated problems due to the perceived dependence on the technology, or technical deficiencies rendering the Smart Home devices useless and uncontrollable. This contrasts with the results of Zeng et al. (2017) where none of the 15 interviewed Smart Home users mentioned availability of device functionality as an asset that might be attacked. Even though not all the participants in our study saw functionality as a target for an attack either, many at least identified the dependence on technical functionality as problematic. Smart Home developers should thus consider designing Smart Home technologies in a way that ensures basic functionality and manual handling of the devices even if the "smart" functions are inoperative due to technical problems.

Privacy and Security Concerns. Participants valued their privacy and security and even hoped to increase the level of security by using Smart Home technologies. However, nearly all participants felt that their data would not be secure in a Smart Home and expressed a variety of concerns related to potential attacks. Similar to the results of Zeng et al. (2017) the physical security theme including measures to increase physical security by using Smart Home technologies but also concerns about electronic door locks and physical access to the home played a major role. Regardless of technical security and likelihood of certain forms of attacks, the users' concerns need to be addressed and may inform risk communication measures. According to Asgharpour et al. (2007) the efficacy of risk communication depends on the alignment between the conceptual model embedded in the risk communication and the user's mental model of the risk. The consideration of prospective user's concerns might thus contribute to bridging the communication gap between security experts and non-experts.

The possibility to control Smart Home appliances remotely appears to be essential for potential users. Thus, even though this would address the users' privacy concerns, a Smart Home concept that only stores data locally within the home and can't be accessed from outside via internet does not seem feasible. Thus, Smart Home developers should explore and evaluate concepts that address the users' concerns: A potential compromise might be to only allow internet access to a limited set of devices defined by the user. Alternatively, the status of some devices might be visible from a distance but not controllable. In a third option Smart Home appliances might only be able to activate an internet connection and contact the user in certain use cases, e.g. when a break-in or smoke is detected at home. After a user reaction to the warning the internet connection would be deactivated again. Future research should investigate the suitability of these options and explore in which scenarios Smart Home functions are perceived necessary to be controlled from a distance.

Acknowledgement

The research reported in this paper has been supported by the German Federal Ministry of Education and Research (BMBF) and by the Hessian Ministry of Science and the Arts within CRISP (www.crisp-da.de/). We further thank Bettina Göbes and Tasja Lutz for their support in the data collection and analysis.

Literature

Asgharpour, F., Liu, D., & Camp, L. J. (2007, February). Mental models of security risks. In *International Conference on Financial Cryptography and Data Security* (pp. 367-377). Springer, Berlin.

Balta-Ozkan, N., Davidson, R., Bicket, M., & Whitmarsh, L. (2013). Social barriers to the adoption of Smart Homes. *Energy Policy*, 63, 363-374.

Borgman, C. L. (1986). The user's mental model of an information retrieval system: An experiment on a prototype online catalog. *International Journal of man-machine studies*, 24(1), 47-64.

Demiris, G., Rantz, M. J., Aud, M. A., Marek, K. D., Tyrer, H. W., Skubic, M., & Hussam, A. A. (2004). Older adults' attitudes towards and perceptions of ‘Smart Home’ technologies: A pilot study. *Medical informatics and the Internet in medicine*, 29(2), 87-94.

Emami-Naeini, P., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L., & Sadeh, N. (2017). Privacy Expectations and Preferences in an IoT World. In *Symposium on Usable Privacy and Security (SOUPS)*. Berkeley, CA: USENIX Association.

GfK, 2016. *Smart Home: A Global Perspective.* CES 2016. Las Vegas, USA.

Green, W., Gyi, D., Kalawsky, R., & Atkins, D. (2004). Capturing user requirements for an integrated home environment. In *Proceedings of the third Nordic conference on Human-computer interaction* (255-258). ACM.

Hekkert, P., Snelders, D., & Wieringen, P. C. (2003). ‘Most advanced, yet acceptable’: Typicality and novelty as joint predictors of aesthetic preference in industrial design. *British journal of Psychology*, 94(1), 111-124.

Jakobi, T., Ogonowski, C., Castelli, N., Stevens, G., & Wulf, V. (2017, May). The Catch (es) with Smart Home: Experiences of a Living Lab Field Study. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (pp. 1620-1633). ACM.

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). “My data just goes everywhere:” user mental models of the internet and implications for privacy and security. In *Symposium on Usable Privacy and Security (SOUPS)* (39-52). Berkeley, CA: USENIX Association.

Malhotra, N., Kim, S., & Agarwal, J. (2004) Internet users’ information privacy concerns (IUIPC): The construct, the scale and a causal model. *Information Systems Research*, 15(4), 336-355.

Mayring, P. (2002). *Einführung in die qualitative Sozialforschung. Eine Anleitung zu qualitativem Denken* (5. Auflage). Weinheim: Beltz.

MAXQDA, *Software für qualitative Datenanalyse*, 1989 – 2018, VERBI Software. Consult. Sozialforschung GmbH, Berlin, Deutschland.

Norman, D. A. (1983). Some observations on mental models. *Mental models*, 7(112), 7-14.

Ogonowski, C., Förmer, D., Gussmann, S., Hennes, P., Hackbarth, K., Jakobi, T., Kersten, K., Läkamp, J., Mengi, A., Pursche, F., Schulze-Sturm, S., Stevens, G., & Wulf, V. (2016). Living lab as a service: Individuelle Dienstleistungen zur nutzerzentrierten Innovationsentwicklung im Smart Home. *WISSENSCHAFT TRIFFT PRAXIS*, 27-36.

Schulze-Sturm, S. (2016). Blickwinkel Smart Home – Studien aus Angebots- und Nachfragesicht. *WISSENSCHAFT TRIFFT PRAXIS*, 5-11.

Shirehjini, A. A. N., Nejad, F. S., Saniee-Monfared, G., Semsar, A., & Shirmohammadi, S. (2016). Mental model development using collaborative 3D virtual environments. In *International Conference on Distributed, Ambient, and Pervasive Interactions* (279-290). Springer, Cham.

Staggers, N., & Norcio, A. F. (1993). Mental models: Concepts for human-computer interaction research. *International Journal of Man-machine studies*, 38(4), 587-605.

Statista (2018). *Penetration rate of German Households in terms of Smart Home technologies*. Accessed from: https://de.statista.com/outlook/279/137/smart-home/deutschland#market-users (7th June 2018)

Stewart, G., & Lacey, D. (2011). Death by a thousand facts: Criticising the technocratic approach to information security awareness. *In Proceedings of the Fifth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2011)*.

Wash, R. (2010). Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (11). ACM.

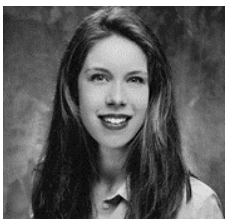
Wilson, C., Hargreaves, T., & Hauxwell-Baldwin, R. (2017). Benefits and risks of Smart Home technologies. *Energy Policy* 103, 72–83.

Zeng, E., Mare, S., & Roesner, F. (2017). End user security & privacy concerns with Smart Homes. In *Symposium on Usable Privacy and Security (SOUPS)*. Berkeley, CA: USENIX Association.

Authors

Zimmermann, Verena

Verena Zimmermann is a researcher and PhD student in the group Work and Engineering Psychology (FAI) of Technische Universität Darmstadt since 2016. Her research interests cover Usable IT Security, Human-Computer-Interaction and Human Factors in Safety and Security. She is especially concerned with user-friendly authentication, nudging in security and privacy and user-centered Smart Home design.



Bennighof, Merve

Merve Bennighof obtained her Bachelor degree in psychology at the RWTH Aachen University in 2017. She is currently a student (M.Sc.) at Technische Universität Darmstadt. In addition to her studies she works in the research group FAI within CRISP since 2017.

Edel, Miriam

Miriam Edel is a Master's student of Psychology at Technische Universität Darmstadt. She works in the research group FAI since 2016 and is especially interested in clinical psychology.

Hofmann, Oliver

Oliver Hofmann is studying psychology (M.Sc.) at Technische Universität Darmstadt. He is looking forward to work in the sector of Human Resources, especially in the field of 'Industry 4.0.'.

Jung, Judith

Judith Franziska Jung is studying psychology (M.Sc.) at Technische Universität Darmstadt. Besides her studies she works in the fields of corporate health management and systemic coaching.

von Wick, Melina

Melina von Wick completed her Bachelor’s degree (B.Sc.) in psychology at the Humboldt Universität zu Berlin in 2017 and is presently a M.Sc. psychology student at Technische Universität Darmstadt. Besides her studies, she currently works as an evaluator and seminar facilitator.

Appendix: Interview Guideline

1. How do you understand the term Smart Home?
2. Which terms do you associate with Smart Homes?
3. Do you use Smart Home technologies? Are you experienced with Smart Homes? If yes, which technologies/devices do you use?
4. What benefits would you personally expect of a Smart Home?
5. How do Smart Homes function according to your understanding?
   a) Open question; Please describe to me in detail how you think Smart Homes function. Please explain your thoughts verbally.
   b) Sketching: Please sketch how you think Smart Homes function and explain your thoughts verbally.
   a)/b) Which components do Smart Homes consist of? How do Smart Home components interact?
6. Do you have any concerns related to Smart Homes? Do you see risks?
7. Which data do you think is secure/not secure when using Smart Homes?