LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
Department "Institut für Informatik"
Lehr- und Forschungseinheit Medieninformatik
Prof. Dr. Heinrich Hussmann

Bachelorarbeit

Privacy Mental Models of Smart Homes

Stephan Kniep
kniepstephan@gmail.com

Bearbeitungszeitraum: 05.09.2019 bis 23.01.2020
BetreuerInnen: Sarah Prange, Karola Marky (TU Darmstadt)
Verantw. Hochschullehrer: Prof. Florian Alt

Zusammenfassung

Da Automatisierung und Energiemanagement aktuelle Themen der heutigen Zeit sind, erfreut sich das Konzept des Smart Home immer größerer Beliebtheit. Um den Komfort eines smarten Zuhauses nutzen zu können, müssen die Geräte des Systems allerdings eine erhebliche Datenmenge erfassen. Diese Daten enthalten nicht nur sensible Informationen der Verbraucher und müssen möglicherweise auch mit verschiedenen Unternehmen in der Branche geteilt werden. In vielen Fällen sind sich Benutzer des Umfangs, in dem die Geräte Aussagen über ihr tägliches Verhalten machen, nicht bewusst. Im Allgemeinen, geben Benutzer oft ihr Einverständnis zu Abwicklungen, die sie möglicherweise nicht vollständig verstehen. Um einen besseren Einblick in das mentale Smart Home Modell von potentiellen Benutzern zu erlangen, wurde eine Studie mit halbstrukturiertem Interview an 15 Teilnehmern abgehalten. Die Ergebnisse geben einen Überblick über die nötigen Schritte, um den Nutzer die ausreichenden Informationen zu liefern, die eine bewusste Entscheidung über die Privatsphäre im Smart Home ermöglichen.

Abstract

With automation and energy management being current topics of the present day, the concept of the smart home is gaining an uprise in popularity. In order to achieve the benefits of such a comfortable home, the systems devices need to collect a vast amount of data. This potentially sensitive information of the consumers could be shared with various organisations within the industry. In many cases users are unaware of the intricacies of how the devices collate data about the consumers day-to-day behaviour and are giving consent to a system they may not fully understand. In order to gain a better insight into the average smart home user, a semi-structured interview study was conducted with 15 participants. The results provide an overview of the necessary steps to provide the user with sufficient information to make an informed decision about privacy in the smart home.

Aufgabenstellung

In a smart home, everyday objects are connected by information, communication and sensor technologies. To provide their services, smart home devices need access to a plethora of data about the users and their homes. To make an informed decision regarding their data, the users require information about the data processing and all entities that interact with it.
(Prospective) smart home users require information to make informed privacy decisions. This information should consider the user's mental model of the smart home device, data flow and entities that can access the data. To gain this understanding, this thesis investigates the mental models of (prospective) smart home users.
Goals:

- Qualitative study of mental models in the context of smart home privacy
- Possible explanation why user do not protect their privacy and why users cannot make informed privacy decisions
- Solutions to adjust the mental models, to provide the missing information or to adjust existing technologies to assist the user

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbstständig angefertigt, alle Zitate als solche kenntlich gemacht sowie alle benutzten Quellen und Hilfsmittel angegeben habe.

München, January 21, 2020

. . . . . .

Contents

1 Introduction

The Internet of Things (IoT) has become a comprehensible concept to the public. Along with self-driving cars and smart cities, the smart home has been part of the consumer market for some years now. While still in its early stages, the smart home industry is already offering a broad selection of devices. The constant expansion of the Internets reach and the increase in bandwidth have built the foundation for networks for collaboration devices, which create and handle data. The concept is built upon an ICT (information and communications technology) network of devices with sensors and actuators [67], which are linked together in order to grant interoperability and automation processes. These devices are usually controlled by a master device (e.g. a smartphone, control interface). The problem lies within the design of these devices without considering the user. Most smart home devices are small sensors connected to the system, that do not give any or very limited indication about their processes, when and what data is collected and what happens with it. Furthermore, early adopters might be unaware of how much data collection is going on, how capable the devices are and how one can control any of these processes. While the concept may create great benefits for the user and generally increases quality of life [17], it also comes with the aforementioned privacy concerns. The large amounts of data which could be collected in such smart environments provides an interesting market for leading IoT companies.

Big technology companies like Google, Amazon, Apple and Samsung started introducing smart assistants, lights, household and other devices for the smart home system (SHS). While the smart home market is currently estimated to have a compound annual growth rate (CAGR) of around 8-15 percent [1, 34, 48, 69], the industry has not reached forecast expectations and is facing data concerns as reports of private data leaks related to IoT applications are published [79, 4, 26]. Overall privacy concerns in europe have increased, leading to the General Data Protection Regulation (GDPR) in 2018. In 2014, Charlie Wilson et al. conducted a thematic analysis of 150 academic publications surrounding smart home and its users which concluded that more focus should be put into user-centered research, *"as a consequence of a technological vision that is struggling to gain user acceptance"* [78, p. 473]. [51] Especially since the concept has reached the mass market, which consequently lead to an uprise of early smart home adoption, actual field studies concerning user perception became possible and should partake in the smart home discussion.

The current problem that arises, is that users do not have the capabilities to make an informed decision about the data they share. The system currently provides limited to no control about the data, created in the smart home. It is built with sensors surrounding the user, who might be unaware of them in their data collection capabilities taking place. Additionally, there is a lack displaying the use of the data and where it is transferred to. The huge amounts of data is potentially send to external entities, where it is not clear, how and why it is processed and with whom it is shared. This lack of knowledge creates serious privacy concerns, that can affect the user. The question remains, what needs to be provided to the user, so that he/she may be capable of making an informed decision about his/her data. Current devices do not provide the neccessary tools for such awareness and do not include an influence from the user perspective.

The goal of this thesis is to explore the perspective of the consumer and potential user towards privacy concerns. Furthermore, the thesis investigates the perceived sensitivity of data and the relation to device benefits. The user trust towards the manufacturer and the approval of privacy trade-offs, that related literature has reported about, is questioned. It contributes to a growing research field, which makes the effort to establish an understanding of the user perception, similiar to previous works surrounding data-transferring technologies, like the Internet [38] itself, Wi-Fi [41] and e-mail encryption [61]. Specifically, the thesis will build upon previous interview studies

in the field. This establishes a broader picture of the mental models of users in regards to dataflow and closely related themes towards current smart home technology.

In contrast to the related work, this thesis is mostly focused on the mental models of non-users of the smart home. Unlike early adopters, they are critical of the current state of the smart home and might even show active resistance [65], despite their interest in the concept. The critical input of non-users can give more insight for future design research which in turn can convince a new audience, while also improving the smart home experience of current users.

First of all, the related work and a conceptual data model of the smart home is found in section 2. Then the three part study regarding the procedure, its participants and limitations is presented in section 3 . The next section presents the results of the included survey, the different mental models of the participants as well as the main themes, that arised in the interviews. The conducted user mental models are compared with one another. The aspects, participants do not know or do not understand (or might not want to understand) are investigated. Participants give possible design recommendations in section 5, followed by a discussion in section 6 regarding the topics of this thesis. In section 7, results will be reflected upon and discussed in a frame, which provides constructive information for future works and development in the industry.

2 Related Work

In this section, the foundational work for this thesis is presented. The benefits of the smart home are introduced and a general smart home data model is established. This is important, so that the user mental models of the participants of the study can be analyzed (4.1). The thesis establishes the general and neccessary parts of a smart home, how they operate with each other and how general interactions are executed. This will allow the comparison to the privacy mental models of the participants and give suggestions for future research. Researcher's concern with security and privacy threats as well as prior research towards the perception and understanding of the user are explored as well. The later sections will build upon the herein presented work.

The literature surrounding the concept of the smart home is vast and scattered around different subcategories. Through the last decades, different names and definitions have been used in relation to the technological advanced home. The definition relevant for this thesis can be fused together from Weiser's concept of ubiquitous computing in 1991 as well as the smart home definition by Aldrich F.K. in 2003. Weiser described a concept of *"hundreds of computers in a room"* which *"will come invisible to common awareness"*. These devices *"come in different sizes, each suited to a particular task"* [76, p 2]. Later the concept was expanded by connecting the devices with the Internet, which Kevin Ashton labeled the "Internet of Things" in 1999. Aldrich F.K. described the smart home *"as a residence equipped with computing and information technology which anticipates and responds to the needs of the occupants, working to promote their comfort, convenience, security and entertainment through the management of technology within the home and connections to the world beyond"* [3, p 17]. New papers have since then built upon these base definitions which was further analyzed by Marikyan et al. [51]. Since the concept has entered the consumer market, the products for the smart home did turn into small computers with sensors and actuators, designed to blend in with the environment, while the system is running at all times.
Described as the third generation of the smart home [51], current devices offer interoperability and a multitude of functions, which are able to collect, transfer and storage data within and outside of the smart home. This described system is the basis for benefits as well as concerns, as such a connected network offers various threats to the privacy of the user.

2.1 Current Benefits of the Smart Home

Throughout the last years, the smart home concept has grown and delivers services in various areas. The concept is able to provide benefits not only directed towards comfort and control through automation and interconnectivity [62, 63], but also in regards to important areas like health, security and energy.

In fact, the first steps of the smart home were focused on supporting disabled and elderly people, to allow a self-determined life with technological support [59, 54]. The smart home gives humans in need of care the chance to live a life on their own. Simultaneously, it offers unobtrusive health control systems with sensors, that can detect critical changes in behaviour [45, 12, 20] or check important health conditions [52, 7]. If neccessary, it is also capable of contacting medical support [49].

The smart home also offers services for the surveillance and security of the own property. The integration of security devices like smart smoke detectors, temperature- and motion sensors allows for cost effective security [5]. Smart home security systems are approached with different protocols like WLAN [14], bluetooth or mobile-based communication standards like GSM (Global System for Mobile Communications) [8], including SMS, GPRS DTMF [37]. These systems keep the user informed about the home status and send potential security alerts over the

phone [5, 71]. This allows the user to investigate the property, be aware of potential intruders or react to security incidents. The current focus has expanded to the security against threats from adversaries, attacking the network [66].

Another key area of the smart home is the potential of sustainability. Network integrated, domestic appliances with sensors like smart refrigerators, dish washers and washing machines create and provide valuable energy information and can be controlled remotely. This creates an energy control system within the smart home, which contributes its fair share of reducing energy consumption [22]. Energy consuming items like lights, kitchen devices, air conditioner, the water heater and more can be monitored in real time and optimized to ensure efficiency [85]. Concepts like iHEM (in-home energy management) have shown to not only reduce consumer costs, but also minimize carbon emissions. Ultimately, internal smart home energy systems will also contribute and help support smart grid technologies like M2M (Machine-to-Machine), which could drastically raise efficiency when it comes to the creation, distribution and consumption of energy in HEMS' (Home Energy Management System) [56]. All these smart home features are made possible through the interoperability and automation of the smart home [60, 44]. In the next section, we will explore the data model of the smart home, which elaborates on the other smart home themes of communication and automation.

2.2 The Data Model of the Smart Home

In the interview study, the participants were asked to establish their understanding of the dataflow of the smart home in a drawing. In order to explore the understanding of the user and in which way it affects the view of their privacy perception, this section first establishes the general data model of the current smart home.

The foundation of the smart home data model is based upon the before mentioned Internet of Things. The core ideas of the concept as of today are (1) devices, which are are able to either create, process, save and share data, interacting with humans or with each other, in (2) an infrastructure of wired as well as wireless networks and telecommunication protocols to interconnect the devices and uniquely identify them in the network. (3) All the data created by the devices, applications and users is running through a high performance network of servers, where it is collected, storaged, processed and managed [32, 81].

IoT devices are creating data with sensors, which sense and detect physical or chemical occurences in its surrounding environment like brightness, temperature, air humidity, pressure, electro magnetic levels but also human body statuses like heart frequency or blood pressure. Sensors build the base foundation of the ubiquitous computing concept, as they capture environmental data, that can be combined and interpreted in a circle of data creation and data processing. The counterpart of sensors are actuators, devices that convert data and electronical signals into mechanical energy (e.g. opening a garage door) or influence the physical environment like changing pressure. The gathered and received information of sensors and actuators is transformed by A/D (analogue to digital) and D/A (digital to analogue) converters [73], allowing analogue in- and outputs to traverse through a digital network.

In order to send and receive as well as manage that digital data, the system requires protocols of identification and communication. Sensors of today have become smart, as they include small memory, are able to utilize data themselves and communicate data within the Wireless Sensor Network (WSN) [35]. The WSN is part of the IoT and works as a subnet, which addresses the individual sensors by its uniform resource name (URN) [32].Similiarly, the implementation of the Internet Protocol Version 6 (IPv6) has enabled the unique identification of all IoT devices in

the Internet. As almost all addresses of IPv4 have been assigned [23] and were limited to 2^{32} adresses, IPv6 eliminates these barriers, as it provides the network 2^{128} unique IP adresses.

Next to identification, the communication within the infrastructure is realised with different protocols and communications standards. The WSN and the internal smart home network or local area network use short range communication standards including wireless protocols like the IPv6 based Wireless Personal Area Network (6loWPAN), Wifi (IEEE 802.11), Z-Wave, ZigBee, Bluetooth, RFID and others [40, 6, 33, 19]. The external network (or Internet) uses Low Power Wide Area (LPWA) communication protocols like Cellular or Sigfox for long distance data transfer. Next to the range, all of these protocols differ in energy consumption, bandwith, frequency and security to offer different environments the right fit. Especially within the smart home system, the data traffic is send not only within, but also in between the different communication networks.

Hubs enable a star mesh communication between multiple devices, while gateways allow the communication between networks with different protocols. They interpret and translate the information of the protocols and enable a network of networks. Usually the home gateway is a router, which connects the local area network (LAN) with the Internet or WAN. This not only allows the interoperability of different devices, but enables the data transfer bridge between the home and external networks (allowing remote control) [64]. Next to the identification and communication of data, the smart home system requires services like the storage and processing of data, in order to create an actual benefit for the user.

The cloud is a network of servers from manufacturers as well as other service companies, who offer storage capacity (cloud storage) and cloud computing, a concept that offers processing power and services like Saas (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) [53]. These cloud services are versatile and flexible, offering fast access to the required storage capacity and processing tools. This gives core functions of the smart home like automation, energy management and monitoring systems the required resources to offer a fluid and adaptable system for the user [15].

The Smart home concept builds upon the idea of automation. Interoperability of smart devices within the home network, has allowed the user to create a system capable of working autonomously. Consequenlty, the system is able to adapt to circumstances and proceed with interactions, that do not require an explicit engagement by user. For example, rather than needing the user to control (turn on or off) the lights with his smartphone upon arrival, home automation allows the light system to react to the unlocking of the entrance door accordingly. The fusion of home automation and the network of Iot even allows this interaction to become invisible. Through the localization of the user's smartphone, the SHS is capable to recognize the distance between the user and the home and corresponds by adjusting the settings (e.g. switch on lights), shortly before the user arrives [30]. To establish a basic but functioning smart home data flow model, it is important to include the entities, which inherently influence the data- transfer, storage, processing, creation and translation. These are the neccessary entities, as previously discussed :

- Sensors/Actuators
- IoT devices (these include sensors and actuators)
- IoT hubs
- Iot gateways
- Cloud servers (for storage and processing)

- Communication network and protocols

Figure (2.1) shows a basic data flow model, including the physical assets neccessary for the system to function. IoT devices can just be sensors, actuators or both and potentially also include internal storage or processing power. Sensors can build a WSN included in the loca area network, which connects the IoT devices of the smart home. The home gateway / router, which are nowadays combined into an integrated access device (IAD) build the bridge to the external network (Internet). External IoT devices like a smartphone can function as a control device, which communicates with the smart home to control and check statuses. Clouds of manufacturers or third parties receive smart home data to storage and process the data for the services they offer. The diagram does not include the informational assets, that do also come in to play, in real world scenarios. These assets include the actual information collected by the IoT devices, log information, user credentials and personal information, smart home status, time and location tracking [39]. Since we are concerned with the data flow understanding of possible smart home adopters, the informational assets are not the focus of this thesis.

2.3 Potential Threats of the Smart Home

The connected smart home and all the objects or nodes within the system could pose several threats to the system. The interoperability between devices also functions between products of different manufacturers with potentially vulnerable sotware implementation.

Some devices are produced with adopted code from software development kits (SDK) offering smart home solutions, which inhibit unneccessary functions as they are build for various different devices. This unused code might include flaws, that could potentially be a threat to the system. Usually Smart home solutions also come with their own cloud services, posing another vulnerable spot. Liu et al. presented design flaws of the widespread, chinese smart home solution *JoyLink*. Flawed authentication mechanisms , missing end-to-end encryption and other design issues lead to sensitive data being exposed to the cloud [46]. Notra et al. [58] disclose potential privacy concerns, which emerge from single smart home devices. Their paper focused on the data transmission of smart home devices like the Nest smoke alarm, Belkin WeMo power switch and the light bulbs from Phillips Hue. Their experiments revealed potential leaks for sensitive data. The data transmission of Nest's smoke alarm revealed a routine communication to a log server, where sensitive data from the various sensors (the smoke alarm inhabits light-, motion-, heat- and smoke sensors) could be sent to. The Phillips Hue smart lights communicate via a bridge to the web log-in. The communication log reveals the bridge's IP-adress, status of each light and username hashes (accounts which are whitelisted in order to control the lights) in plain text. This shows, that not only sensitive data can be accessed, but the status of the lights can be manipulated from outside attackers, if they are able to eavesdrop a datatransfer between a user and the smart lights. The WeMo products (WeMo Motion and WeMo Switch) also revealed data via plain text. Furthermore, the control of the WeMo Switch does not require authentication, which means no method is put in place to legitimize a request, which allows unauthorized manipulation. Next to the devices, software applications for a SHS was also found to be insecure.

Fernandes et al. [24] analyzed Samsungs programming framework SmartThings and applications build upon it. They were able to identify an overprivilege for applications, either by requesting operation rights, which are not neccessary for any operation or applications simply being granted rights, which were not requested from the user. This overprivilege could potentially be abused by phishing applications (e.g. a battery application eavesdropping for smart lock pin codes) pose security and privacy threats for the user. Among other standards, data transfer in the SHS is being transmitted via the wireless communication protocols Z-Wave and ZigBee. These protocols were

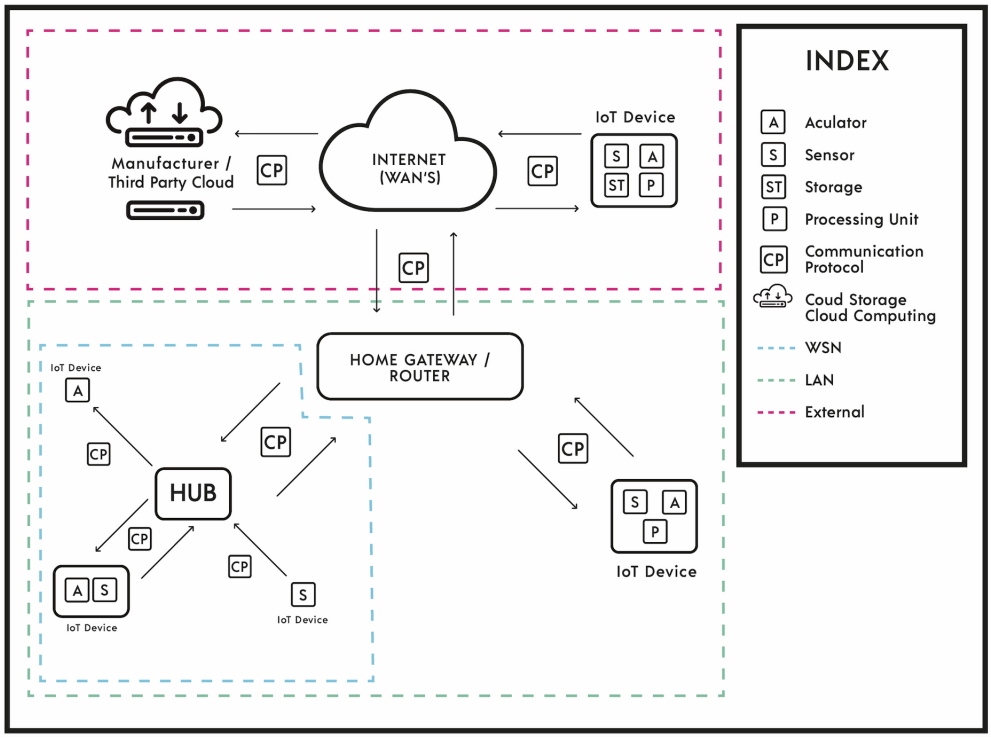

Figure 2.1:

SHS data flow diagram showing the physical assets of the smart home network [29, 39]

also identified, to have serious security breaches. Fouladi et al. demonstrated a way to intercept unencrypted packets, which are sent between the controller and the devices, allowing them to get access to sensitive data [25]. The ZigBee protocol potentially allowed intruders to breach into the system, compromise the active network key (due to the protocols use of a default link key) and gain control of all devices in the network [47].

This section has presented different real life cases, which show, that all parts of the SHS can and do have issues regarding security, rightfully raising concerns within the research. While certain flaws of specific cases in the presented research may have been secured and fixed, it does not invalidate the raised concerns of possible threats in the individual areas (devices, applications, transfer protocols) of the SHS. The security concerns consequently imply, that the privacy is also at risk.

Similiar to the smart home, there is no consensus, when it comes to the definition of “privacy”. Encouraged by the mass distribution of news papers and the initiation of photography, Samuel Warren and Louis Brandeis published the article “The Right to Privacy”, in which they defined the term as the *“right to be let alone”* in the year 1890 [74, p 1]. Alan F. Westin described a first definition of privacy in regards to personal information or data, saying that individuals determine for themselves when, how, and to what extent information about them is communicated to others [77]. Shortly after, the first data protection laws were passed in Sweden (1973) and then in Germany (1977), regulating the collection and transfer of personal information. In the wake of the Internet, ubiquitous computing and “always online” functionality , the discussion surrounding information privacy has gained importance again. While the market has continued to grow and every device is collecting data, the industry has not seen any implementations of

specific regulations or standards, which deal with these concerns. This has shifted the research towards a user focused approach, especially concerned with the perception of the user, in order to lay the groundwork for the future of the industry. Surveys of several publications have underlined a general concern of private home data being shared with the outside world, but also unveiled that there are many different privacy positions demanding a more nuanced research.

2.4 User Perspective

A few years ago, the research of smart home and all its related topics consisted mostly out of technical related papers, far outnumbering any other topic of interest [68]

Literature [13] started to point out, that research described the benefits of the technology (product centric approach), while ignoring the users viewpoint. This thesis is concentrated on the exploration of user perception in a qualitative and nuanced approach, contributing its share to the research of user interviews regarding the smart home as well as the privacy discussion that comes along with it. Research towards user mental models of smart homes, as well as research about influencing factors within the mental model literature are taken into account. The growing user centered literature started with device specific user studies and later also moved to towards broader SHS user understanding and perception.

In 2016, Worthy et al. [80] have expressed the importance of including human values into the discussion of the IoT technology, in order for people to adapt and accept the connected IoT systems in their life. In their work, they developed a device with multiple sensors, which was placed in the homes of the 5 recruited participants, without educating them about the specific data, that was collected by the device. The qualitative results of the study unveiled how quick a new device, even with signs of presence, can recede into the background and is overlooked by the users. Purpose of the device and trust towards the manufacture of it (or in this case, the distributor) has a big influence of the trust relationship between user and device. Despite of potential worries, devices with an intentional design to blend in with its environment, could be forgotten although concerns towards it might not have changed.

Just three years ago, Clark et al. claimed to have released *"the first substantial public corpus of end-user descriptions of desirable IoT applications"* [16, p 44:3]. The paper explores the potential priming (influence of prior experience and perspective on newly received knowledge [72]) of end user's mental models, caused by the various smart home abstractions, which could lead to distorted results of researchers without realisation. In the included study, the 1,500 participants received one of four invidividual questionnaires, each giving a different depictions of the same smart home concept, in order to discover the impact these different depictions can have on the participants mental model. The individual models show different results and underline the significant influence of priming.

In conclusion, priming needs to be seen as a crucial feature of smart home research. It *"influence[s] the kinds of interactions that users will task the system with"* [16, p 44:15], while users will in turn shape the services of the system. The conclusion of these findings demand a greater focus on priming, not only as an unconcious influence, but as a tool to understand and guide the technology and the behaviour of the user. The interview of the thesis was structured accordingly to detain additional influence and discover current industry priming on user mental models, while also acknowledging the non preventable priming by the structure of the interview. As the survey included privacy specific themes, like the IUIPC questionnaire, it just be noted, that participants were confronted with potential priming before the actual interview.

The work of Lau et al. [43] was one of the few, that pays attention to the consideration of non-users and explores their understanding and perception towards the device. Focusing on privacy perception in regards to smart assistants like the Amazon Echo and Google Home. They conducted a user study of 34 participants, half of them non-users. The direct comparison of the demographics unveiled a marginal difference in privacy concerns. Non users were sceptical of the companies and their compliance of the terms of service (ToS), while early adopters generally dismissed data collection concerns, as they *"already give them so much information"* and *"don't think a little bit more matters."* [43, p 102:12]. Next to non-users, who do not and the users who do approve of the privacy-comfort trade-off, the rest of participants were not aware of any trade-off being in place, when purchasing a smart assistant. Next to the concerns of data collection, data sharing with third parties and lack of utility of the device were the factors against an investment. The results of this paper, especially regarding non-users, discovered a range of concerns are essential, however it focused on a specific smart device case with audio recording functionality. Audio and video recordings are the most privacy sensitive data sources and might not reflect the concerns of the general smart home system [55, 84].

The first research regarding end user mental models of smart homes, specifically established with the sketching technique, was established by Zeng et al. in 2017 [83]. The study with 15 longtime smart home adopters explored their privacy, security and multi-user concerns . Despite being aware of some privacy threats, user concerns were more focused towards security threats and conflicts with other users of the smart home. The recurring theme, that participants think the privacy trade-off is *"just part of big data"* [83, p 71] does not align with the study results of this thesis. This general outcome was further supported by a similiar research paper from Tabassum et al. [70]. The paper further elaborates the conflict of the privacy trade-off, as people generally tend to trust a system, so long as it did not produce critical events yet [80]. Furthermore, the convenience of the products puts privacy and security risks in a contrast, where they become *"too low to trigger any actions"* [70, p 435]. Overall users were aware of audio recordings, but were not concerned with it. Some participants show concern, especially when the device shows potential signs of activity, but generally data collection is seen as something rather positive. Despite the general acceptance of these privacy concerns and repeating talking points like trusting the company [83, 43], accepting the trade-off and not feeling like a potential target, participants did advocate for more transparency, even enforcing consumer protection laws.

Different demographics and cultural differences in the related work do seem to have a critical influence on general study results. The majority of the related work concerning user perspective has been conducted in the United States of America [70, 83, 84, 16, 82] and shows a general acceptance of the privacy trade off. The research established in Germany shows different results regarding the privacy perception. Zimmermann et al. conducted a semi-structured interview with 42 participants with various degrees of smart home experience. Participants were allocated to either describe their mental models of the smart home through verbal explanations or sketching. The results of this paper are closely aligned with the one's from this thesis. Almost all participants (39 out of 42) declared, that their data was not save. Generally participants had an adequate understanding of how the system functions. User experience and technical knowledge did generally not create vastly different results. Possible functionality and general mental models seemed to be aligned with advertised and popular smart home devices. While conducted as a semi-structured interview, the results did unfortunately not reveal the opinion of the participants as citations and possible feedback of the users were almost not included in the paper. The possibility of restrictions towards smart home connectivity with external entities was mentioned, but not seen as something viable, as many of the participants mentioned remote controls as a key smart home feature. On the other hand, a quantitative study of 942 participants regarding privacy risk perception of various use cases (smart home, smart health devices and social media). The results listed data collection

and data analysis as a less severe concern. While the mixing of these different scenarios and the framing of the questions (even mentioned in the paper) did provide contradictory results, the perception of smart home privacy is rather mixed. While the severity might alternate, most research still points to users advocating for more transparency surrounding data collecting and usage.

2.5 Summary

Smart home literature is broad, providing insights into various topics of the concept. As the industry around it continues to grow and has entered the mass consumer market, the literature explored other perspectives, namely technology-centered research. As more and more users adapt to a SHS, research towards the user experience has grown. Prior smart home studies, which focused on user mental models, delivered the ideas, on which this thesis is based upon. Until now, user research has generally been focused around consumers, who are already smart home adopters. The related work, that did include non-users, did not focus on their particular perspective. Since all related research for this thesis did not contribute a focused investigation of it before, the conducted study was especially focused on potential smart home users, who have not yet invested into the technology, or only to a small degree.

The pool of potential smart home users gave a unique outside perspective towards the current smart home perception. Especially the mental model of non smart home users are of interest as they can guide the understanding of a system. Bibby and Payne's work about device learning made the case, that an original mental model could potentially influence the way a user incorporates new knowledge to his understanding of a system, even if that mental model was formed before an actual interaction with that system [9]. The results of this thesis give an inside into the mental model of potential user, which was formed through advertisement by the indusrty and development of the products, that have reached out to people with a basic interest towards that technology.

3 Study

This section presents the approach of this thesis' study, including the neccessary items for the study, how it was conducted and information about the participating interviewees.

3.1 Apparatus

Before the recruitment of the participants, one pilot interview was conducted, in order to estimate the length of the study and modify the execution and structure of the interview, especially the drawing section. The pilot interview was not included in the results of this thesis. The following items for the study were used: All interviews were recorded with a Tascam field recorder (audio recordng) and an Iphone (audio- and video recording). Seven interviews were held at the Institute of Pathology of the Ludwig-Maximilians-Universität München. The rest were held at the apartments of the participants in munich or at a neutral apartment in Berlin.

3.1.1 User Survey

The survey contained three separate topics, including general information (demographic) including an affinity for technology interaction questionnaire (ATI) [27], the 10-item IUIPC questionnaire, introduced by Maholtra et al. [50] as well as a self-created data sensivity questionnaire (3.2), containing 18 questions regarding participants perspective on certain data sensivity. The survey was constructed via the online open source tool LimeSurvey from the LimeSurvey GmbH. The survey was held at the start of every interview. Participants were provived with a Macbook laptop, on which the survey was running on.

3.1.2 Drawing exercise

The user mental model section required the participants to create a drawing of the smart home data flow understanding. Participants were provided with A3 paper, two sketching pencils and three color pencils in order to highlight certain areas relevant to the interview questions. Prior to the drawing exercise, participants were provided with a smart home device pool of 24 smart home devices, categorized in different themes (3.1). The devices were previously selected and printed on paper, cut out to small items and sized accordingly to the provided paper.

3.1.3 Semi-structured interview

The interview went by a prescribed questionnaire including 15 questions and three scenarios, while also following up on answers and start open discussion. Some interviews drifted off to sub topics, allowing the participant to elaborate on points, describe experiences or adding sidenotes. Essential answers and opinions were further explored by the researcher.

3.2 Procedure

Participants who signed up to the interview via the scheduling site doodle, were able to choose an appointment of the free slots, that were setup during a two week period. The rest of the interviews were either held in the home of the researcher or the participant. The invitation mail included the address and room location of the interview space. The whole interview was recorded by an external audio recorder and was further video-recorded, starting from the drawing exercise. Particpants received an information paper about the data collection and were asked to read through and sign a declaration of consent.

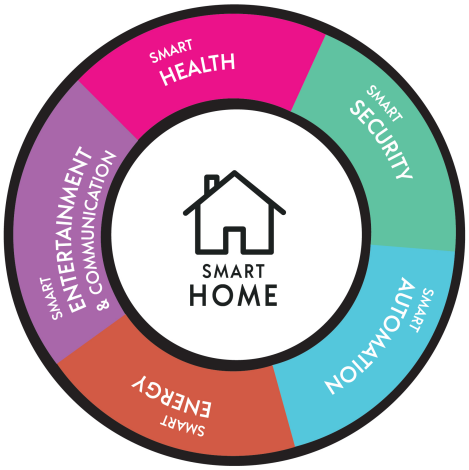

Figure 3.1: The smart home devices of today, can be categorized into 5 themes [31]

The interview started with the survey, which the participants answered via a computer contributed by the researcher. The survey started with general questions about the participant and an ATI (affinity for technology interaction) questionnaire, that is concerned with the participants active engagement in technology interactions. Participants were then asked to name any smart devices they already own, if any. The survey continued with the 10-item IUIPC (Internet User's Information Privacy Concerns) questionnaire, which focuses on the general user perception and compliance towards the *"collection, control and awareness of privacy practices"* [50, p 338]. The survey was completed upon evaluating the sensivity of 18 personal data sets, which may possibly be collected in a smart home environment 3.2.

Upon completion of the survey, participants were asked to conduct a drawing, representing their understanding of the data flow of a smart home. Similiar to the method of other user-centered literature, which was discussed in the related work section [70, 83, 38], this meant to visualize the data nodes and their data transfer connections to each other. The participants were told to include any relevant entity to the model, that in some way or form was thought to be included or related within the dataflow system.

All participants were presented with a pool of smart home devices (n=24), which were divided into five subcategories. The categorization followed the classification of a study by Splendid Research [31], including "Entertainment and Communication" (devices included: smartphone, smart assistant, smart hub, smart speaker, smart TV), "Energy Management" (devices included: smart lights, smart heating, smart plugs, smart water meter, smart electricity meter), "Security" (devices included: smart smoke detector, smart surveillance, smart doorbell, smart lock), "Health"(devices included: smart watch, smart brush, smart matress, smart blood pressure) and "Automation"(smart vaccum, smart jalousie, smart fridge, smart thermostat, smart coffee machine) (3.1). It should be acknowledged, that these categories might vary in the literature, as slight distinctions in category definitions were found [10, 18]. One device was selected per category, reaching a total of five selected devices, as a basis for participants to start.

The drawing was done in combination with the Think-Aloud technique : Participants were asked to verbally describe their drawing procedure, including any thoughts related to the topic. Once they felt the drawing was in accordance with their understanding of the system, the interview

continued with questions related to the system, that was drawn. If the participants mentioned any new entities in the on-going interview, which they had not included in their drawing, the researcher would ask them, wheter or not they would like to include the mentioned entity within the system. This makes sense, as some people might see certain entities as self-evident. Next to the questions related to the transfer, collection and creation of data, participants were asked to describe a specific interaction and the dataflow that comes with it and which entities are included.

The discussion continued with the meaning of the term “smart”, when and how the participant has conciously heard about the smart home and if he/she has used any smart device yet. Since most of the participants did not have any smart home devices yet, they were asked for any specific reason of not investing into the technology yet. Furthermore it was discussed, what are comprehensible reasons to decide for or against a smart home. The discussion was then guided more towards privacy, data sensivity and the future of the industry. Participants were asked about sensivite and non-sensitive data (following the questions of the ATI questionnaire) as well as the relation to comfort, which could generally explain the privacy paradox [57].

Before the last section of the interview, the participants were asked about any part of the smart home system, that is not clear to them or where they wish to receive more information about as well as their direct feedback to the smart home industry, what they wish to see the industry do in the coming years.

The end of the interview was focusing on three specific smart home interactions focused on a smart vacuum-, a smart fridge- and a smart light interaction, where the participants were asked to once again try and describe the data flow, what data is used in the specific cases and where they see benefits and concerns within the scenarios. Upon completion, the participants had a last chance to add anything to their drawing and were asked to fill out a confirmation formula, in order to receive their selected compensation. The semi-structured interview questions can be found in Appendix A.1.

3.3 Participants

As eloborated in prior sections, the recruitment was specifically targeted towards potential smart home users, with no or a limited amount of up to three smart home devices. An invitation with an introduction of the topic and procedure of the interview was sent via the info service mail of the Ludwig-Maximilians-Universität München. Participants were able to respond to the invitation by signing up on one of the interview appointments, which were set up via an online scheduling site (doodle).

Out of the 15 participants who signed up for an appointment, two individuals cancelled the interview, while five others did not show up to the appointment. These seven missed interviews were later replaced with participants, who were recruited via Facebook groups related to media computer science as well as related people of the researcher. A total of 15 participants were recruited and finished the interview. 12 of them were male (n=3 female) and all interviews were held up in the German language. 8 students, 5 self-employed and 2 employed workers participated, while 4 of them specified to have a background in computer science (web development, IT and HCI). The youngest participant was 18, while the oldest was 64 (mean = 35,73.. ; SD = 14,78). 12 participants do not live alone (with family = 5; flat share = 3; living with partner = 3), while 3 do.

There was a total of 4 participants, who stated to have atleast 1 smart home device, another one affirmed to have a smart home device and named the smartphone. While the smartphone itself is

Question/ Participant	i	ii	iii	iv	v	vi	vii	viii	ix	x	xi	xii	xiii	xiv	xv	xvi	xvii	xviii	M	Med	SD
1	2	2	0	1	3	1	1	2	3	1	1	2	1	1	1	1	3	3	1,61	1,00	0,89
2	2	3	3	3	3	2	3	2	3	2	3	1	2	2	3	2	2	2	2,39	2,00	0,59
3	1	2	0	0	3	0	0	3	3	3	1	1	1	1	2	2	2	2	1,50	1,50	1,07
4	3	0	1	0	3	2	1	2	3	2	1	1	2	2	1	1	1	2	1,56	1,50	0,90
5	2	0	0	0	0	0	0	0	3	3	3	0	0	0	3	0	3	3	1,11	0,00	1,41
6	0	3	2	0	3	1	1	3	3	2	1	1	2	1	1	2	2	1	1,61	1,50	0,95
7	3	0	0	0	3	2	1	3	3	3	2	1	1	1	1	2	2	3	1,72	2,00	1,10
8	1	1	2	1	3	1	2	3	3	2	3	1	2	2	2	2	3	3	2,06	2,00	0,78
9	1	3	2	3	3	1	2	1	3	2	2	2	2	1	1	1	3	1	1,89	2,00	0,81
10	1	2	0	1	3	2	1	3	3	3	3	3	3	3	3	3	3	3	2,39	3,00	0,95
11	1	2	2	1	3	2	2	3	3	2	3	2	2	2	3	2	3	3	2,28	2,00	0,65
12	1	2	2	3	3	2	3	3	3	3	3	2	2	2	2	3	2	2	2,39	2,00	0,59
13	1	3	2	2	3	2	2	3	3	2	2	1	1	1	2	1	2	1	1,89	2,00	0,74
14	1	3	3	2	3	2	2	3	2	3	3	2	2	3	3	3	3	3	2,56	3,00	0,60
15	3	0	0	1	3	0	0	2	2	2	3	3	3	3	3	3	3	3	2,06	3,00	1,22
Mean	1,53	1,73	1,27	1,13	2,80	1,33	1,40	2,40	2,87	2,33	2,27	1,53	1,73	1,67	2,07	1,87	2,47	2,33			
SD	0,88	1,18	1,12	1,18	0,75	0,79	0,95	0,88	0,34	0,60	0,85	0,81	0,77	0,87	0,85	0,88	0,62	0,79			

Figure 3.2: Results of the data sensivity questionnaire show, that out of the 18 data sets, visual and biometric data is seen as most sensitive (v. surveillance camera footage, viii. photo album, ix. biometric data) ; P5, the only participant, who was specifically okay with the collection of data for comfort, rates most of the data as “not sensitive”. (For actual data sets, see A.4)

included in the smart home network (and was also included in our pool of smart home devices), the smartphone alone was not considered as a specific smart home device, as other smart home devices need to be integrated in the system, for it to become one.

Participants affinity for technology (ATI) [27] was measured by the corresponding questionnaire in the survey and resulted in a mean of M = 4.07 (SD = 1) out of a seven point Likert-scale (0-6). While this is a quantitative study and these measures are not significant for broader research, the average ATI score of the individual models (4.1) align with the general implication, that a lower ATI score tends to imply a simpler mental model. Participants with a limited model (6 participants) sit at M = 3.41 (SD = 0.9), while the average score of the basic model (7 participants) results to M = 4,24 (SD = 0,77) and the critical model (2 participants) to M = 4,67 (SD = 0.33). The followed up IUIPC 10-item questionnaire, which is concerned with the general privacy concerns of the participants [50], measured a mean of M = 5.9 (SD = 0.57) out of a seven point Likert-scale (1-7).

3.4 Limitations

Due to the nature of the interview and the selected focus group, the study has the following limitations :
As this thesis tries to explore the perspective of non smart home owners and potential future adopters, participants can only present concerns and opinions about the smart home system built on technical knowledge, received news about the topic and related ones or incidents in which they interacted with such system (except three participants, who did own smart home devices). It must be pointed out though, that these limitations come in exchange for valuable data concerning consumers who are interested in the product, but have not yet invested for given reasons.

Participant	Age	Sex	Employment	Field of Work	CS Background?	Living Situation	Duration
P1	25	male	student	web development	Yes	living with partner	46:00
P2	24	male	student	archaeology	No	living with family	47:00
P3	28	male	student	human medicine	No	living with partner	37:00
P4	18	male	student	IT	Yes	living with family	41:00
P5	25	male	student	German as a foreign language	No	living with family	53:00
P6	27	male	academic worker	education and research	No	living in a flat share	58:00
P7	23	male	student	HCI	Yes	living in a flat share	1:13:00
P8	64	female	self-employed	event organisation	No	living alone	1:25:00
P9	61	female	self-employed	real estate	No	living alone	1:13:00
P10	26	male	student	business economics	No	living with family	58:00
P11	59	male	self-employed	event management	No	living with partner	1:44:00
P12	37	male	employed/self-employed	IT administration	Yes	living with partner	1:08:00
P13	32	female	student	medicine	No	living in a flat share	1:23:00
P14	37	male	employed	event organisation	No	living alone	1:00:00
P15	50	male	self-employed	event management	No	living with family	44:00

Table 3.1: Participants demographic (Age mean = 35.7, SD = 14,78 ; Interview duration mean = 1:02:00, median = 58:00)

The questions of the interview were constructed in a way, that would not implicate certain dangers or risks, in order to not affect the answer or imply a right way to respond. This approach tries to prevent further influence and only reveal current priming (as discussed in 2.1.2) of the industry, towards non smart home users. While the questions were asked in this cautious manner, it is important to notice, that the survey was conducted prior to the interview. Next to the ATI questionnaire, it also asked about the data sensivity of certain scenarios and included the 10-item IUIPC questionnaire, which is about the attitude towards sharing data and private data rights. This could have predetermind a mindframe for the participant, in which the interview was conducted in. It is possible, that the structure of the interview did have an effect of the general framing, as the results of the thesis do lean towards a majority of privacy concerns.

The interview studies were held in-person and was limited to a specific demographic. Participants were either recruited through the info service mail of the Ludwig-Maximilians-Universität München or acquaintances of the researcher (from munich and berlin), which might give narrow results in regards to opinions towards the study. However, these limitations should not distract from the valuable results, that were made with this study. It is important to use the qualitative results as the basis for quantitative studies, focused on a more balanced demographic.

4 Results

As the research regarding user perception towards the smart home system and industry is scarce and incomplete, the goal of this thesis was to further explore the understanding and concerns of a research group, that was not yet adressed.

Much like Wash and Renauld et al. [75, 61] this qualitative study concentrated on a thematic analysis after Braun and Clarke [11]. It does not report how many users alluded to each of the explanations in their statements, but rather showcases the themes occured in the interviews. The audio and video recordings of the study were transcribed and analyzed. The average duration of the 15 interview was 62 minutes (Med = 58 minutes). The themes included in the results follow two different approaches (top-down and bottom-up approach) : 1. The task of this thesis laid out the framework for the base themes. These core topics were further explored in related work and formed the interview questions, that set the main themes for the thesis. 2. Subthemes and related topics were additionally found in the analysis of the interviews. Through a bottom up coding method, the interviews were scanned and possibly relevant statements given by the participants were noted down and described with short sentence subcodes. 146 individual subcodes were collected from the interviews. In an iterative process, similiar subcodes merged to the overall codes of the study, which were then sorted into the themes, which give a representation of the topics that came up. Any quotes of the participants were translated from the original language (German).

Device Category /Participant	**Health**	**Security**	**Automation**	**Energy**	**Entertainment and Communication.**
P1	Watch	Door/Window Sensor	Jalousien	Lights	Voice Assistant
P2	Brush	Smoke Detector	Smart Fridge	Lights	Smartphone
P3	Watch	Smoke Detector	Vacuum	Lights	Voice Assistant
P4	Matress	Surveillace	Smart Fridge	Lights	Speaker
P5	Watch	Lock	Jalousien	Lights	Voice Assistant
P6	Matress	Lock	Thermostat	Plugs	Voice Assistant
P7	Watch	Doorbell	Vacuum	Lights	Smartphone
P8	Brush	Doorbell	Vacuum	Heating	Smartphone
P9	Watch	Door/Window Sensor	Jalousien	Plugs	Smartphone
P10	Brush	Smoke Detector	Vacuum	Heating	Smartphone
P11	Blood Pressure	Surveillace	Smart Fridge	Heating	Smart Hub
P12	Watch	Surveillace	Vacuum	Lights	Smartphone
P13	Brush	Smoke Detector	Thermostat	Lights	Smartphone
P14	Watch	Surveillace	Vacuum	Heating	Smartphone
P15	Watch	Smoke Detector	Thermostat	Plugs	TV

Table 4.1: Individual device selection of the participants. The devices were used for the drawing exercise of the mental models. (To save up space, the “smart” attachment was removed. All devices are smart and compatible for the smart home system.

Entmt. and Comm.	15	Automation	15	Security	15	Energy	15	Health	15
Smartpone	8	Smart Vacuum	6	Smart Smoke Detector	5	Smart Lights	8	Smart Watch	8
Smart Assistant	4	Smart Blind	3	Smart Surveillance	4	Smart Heating	4	Smart Brush	4
Smart Hub	1	Smart Fridge	3	Smart Doorbell	2	Smart Plugs	3	Smart Matress	2
Smart TV	1	Smart Thermostat	3	Smart Lock	2	Smart Water Meter	0	Smart Blood Pressure	1
Smart Speaker	1	Smart Coffee Machine	0	Smart Door/Window Sensor	2	Smart Electricity Meter	0	-	-

Table 4.2: Total quantity of the smart devices, selected by the participants (for the drawing exercise)

4.1 Smart Home Mental Models

Participants were asked to visualize their understanding of the smart home data flow in a drawing, consider all entities in the system and think about the transfer, collection and creation of

data. The participants were provided with a selection of smart home devices, put in five different categories (Smart Health, Smart Energy, Smart Automation, Smart Entertainment and Communication, Smart Security). They were asked to choose one device per category and integrate them in their drawing (4.1). Similiar to related work, the drawings showed different levels of knowledge regarding the smart home system and all factors that come in to play [70, 83]. Therefore, the drawings were divided into three categories, based not only on the drawing itself, but also on what was said during the drawing and interview afterwards. While the different categories generally distinguish themselves due to the fidelity of the drawings, some participants with little to no technical knowledge were able to name important parts of the system and more knowledgable participants missed parts of the system. Despite advising each participant, that nothing in the model is self-evident (and hence may be included in the drawing), some participants might still have seen certain parts of the system as self-evident. If these were mentioned verbally, but not included in the drawing, the participants were asked whether or not they want to include it in the drawing. This intervention was only done, to compensate for missing key nodes out of self-evidence.

4.1.1 Limited Data Model

Participants with a limited model (6 participants) (4.1) were not confident about data connections between devices. Usually no network specific devices like a router or a hub were considered, however some participants did acknowledge a center device in the system, connecting the devices, working as a gateway to the external network. Most were also mentioning one general device within the system and generally either picked the smartphone or the smart assistant as a control hub. The external network was not further elaborated on. Throughout the interview, participants did eventually mention some information going outside of the smart home or even mentioning a storage or server and the manufacturer being involved. Otherwise the connection to the outside world seemed abstract. Participants described direct WLAN connections to the server or external devices. Some did question connectivity to WLAN due to distance, but were not able to explain other possible connections, only that radio masts are somehow involved. Communication between devices was happening via WiFi or WLAN, some participants mentioned direct communication with Bluetooth. Sometimes the communication between devices was made with the use of an app. The connectivity understanding to the app was also fairly limited. P5 did differentiate between an Internet connection and a connection via an app. P8 for example, described a direct interaction with a smart toothbrush and the corresponding application on the smartphone, but was unable to further explain how they are connected : *"And then they're connected somehow. But I don't know how it gets there."* (P8). That the app does receive the information, processes it and sends it back to the brush is clear, although it is not mentioned, that for the data to be processed, it leaves the phone. In the interaction, if any at all, the duration of the connectivity is also questioned, because of the duration of the service (in this case, brushing your teeth):*"It must be connected all the time then, I don't know."* (P7)

As related work has previously shown [70], these limited models seem to be oriented about the

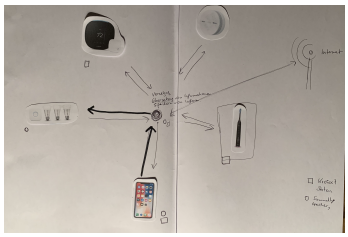

Figure 4.1: limited model

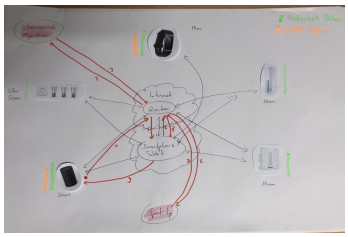

Figure 4.2: basic model

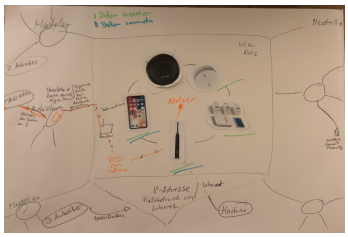

Figure 4.3: critical model

service itself, without seeing the possibility of the device communicating with the network, despite of no direct user commands. Next to the direct connections of the devices to the phone, P2 also mentions conditional interoperability between devices : *"The devices may also be able to interact with each other [...]. That when I brush my teeth, the lamps go out 10 minutes later."* As mentioned before, participants may mention a storage or a server, but the understanding of it and how it interplays with the devices is very scarce, at times contradictory. P2 describes an interaction with the smoke detector, in which the alarm goes off and the information goes through the server, explaining that the server is neccessary in order to save the data. Upon asking, wheter or not the server is incorporated within the system, P2 responds: *"Not necessarily. Well, if it works over Bluetooth, I don't think there's a server to store it on."* In contrast to the described communications, P13 did only see connections between devices possible, if they traverse a center device, that receives all the data: *"Of course it needs another place, except the smartphone and the lights [...]. A place, so to speak, that connects all the information. So a smartphone alone and a light would not be enough."* Most participants with a limited model tried to include the technical terms and functions they know, without neccessarily understanding the relation it has within the system. P5 put a strong emphasize on processors and encryption, while missing critical parts of the system. Definitions of words were also unclear, as the participants used the "Internet" to describe connections as well as data banks or computing power services of the Internet. Simple devices, that do not require specific, external services were believed to not be connected to the Internet. P4 also centered the phone as the main control devices, mentioning it as a neccessary bridge of devices before going to the Internet: *"Then it goes from the fridge to the mobile phone from the mobile phone to the app and then back again [to the phone], so that you confirm it and then back to the fridge."* Particular comments showed logical knowledge of the participants, while being unable to translate it to the technological field. P13 for example mentions the neccessity of gateways (while not using that specific term) to combine different systems: *"Because I think this device [smart lights bridge] can only do certain... so it is almost always coupled with a certain system, there must be some kind of translation, because it is a different system than that [of the smartphone]."* Overall, participants were heavily focused on service oriented connections of the data flow. Core entities and features of the smart home were mentioned, but merging them into a system was the barrier. However interoperability is expected to be possible and external entities are vaguely mentioned. Therefore, participants did have a vague idea of how the system functions. The core problems of this mental model is how the general data flow functions and which entities are involved at what time. Almost no threats within the data model are mentioned, besides data collection and potential unavailability of the system (not caused by an attack, but due to some error).

4.1.2 Basic Data Model

The basic model (7 participants) (4.2) generally captures all key parts of system. The communication of the devices with each other works via a central home router, which functions as a gateway to the Internet. Servers of the manufacturer receive the data created by the smart home, where it is analyzed and the results are sent back. The general communication is mostly described as a two way communication, meaning a constant back and forth of data transfer between communicating devices. Participants recognize, that some devices mostly function through the services, that are offered from external sources: *"Much of what we see here, what is called smart, is actually just a query of databases."* (P12). Interconnectivity and data sharing purposes are described more clearly than in the limited model.

Next to external control of the smart home, participants mention, that data of one device can potentially give another device input in order to react accordingly: *"It [smart heating] works with a thermostat, for example. It gets information from there and then switches its calorific values*

up and down accordingly" (P11). Generally, the focus is particularly on devices communicating with each other and reacting to one another, rather than just delivering services of their own. P7 mentions, that the smart home should be capable to track the movement patterns of the user: *"That's what makes a smart home for me. I leave the living house, trusting that it will be economical and preferably switched off [...]. And when I come back, it should look exactly the same as before."* Participants did mention, that the manufacturer as well as third parties, related to an interaction, do receive information, as all companies have to be contacted for the services that are included.

Besides data leaving the smart home, participants mentioned data, that is also externally stored in a data base, so devices can compare and adapt. P6 mentions the smart assistant, which tries to adapt to the user's voice: *"And sometimes it's a little indistinct, when you ask Alexa and say "Hey, turn off the light!" And she asks three times which lamp it actually is, that's where the voice is adjusted in the background [...]."* Additional features, like the online service IFTTT (If This Than That) and the inclusion of API's (application programming interface) are mentioned by the participants, who were in possession of some smart home devices (P3, P6).

During the drawing, participants already started reflecting on potential concerns or threats, as they thought about the data flow between network nodes. Unlike participants with the limited model, participants mentioned hackers and flaws of the system and see them as possible, real world threats, that are to be considered. While there is still some uncertainty about what data is leaving the smart home and which devices might only communicate via the home network, participants are capable of describing more complex analysis of single data communications: *"So the lighting system at home reacts based on the data that the mobile phone continuously sends to a cloud via an app, which in turn is authorized to record GPS data, and the device is previously configured so that when a person reaches a certain GPS position, it is activated."*(P7). Despite the familiarity to some technical terms that play a role within the smart home, the core understanding of the data flow was similiar between smart home device owners and the participants without any experience.

4.1.3 Critical Data Model

Two participants did expand the understanding of the data flow to a second order. These were categorized as a critical model (4.3), in which the data flow can also leave the framework of the service and expand to special interests. Participants did generally have a more critical view towards all aspects of the system. The manufacturers are constantly collecting data of the devices, analyzing and also saving the data in their storage. External entities like hackers and other third parties were included in the data flow model. Both participants described the data flow as a trace of data, you leave behind when interacting with the Internet. P10 did even aquire a smart assistant, but eventually unplugged the device, because of privacy concerns. The data of the user were believed to be shared with marketing companies, to deliver a service for the manufacturer and sold to various companies, which use the data for their own benefits. The government was also seen as an entity, potentially collecting data of the smart home. In general, these models did not necessarily built upon the previous models. The core data flow of the devices within the home was neglected for a focus on the external part of the system. P10 was taking more time to describe a network of smart homes, which all contribute to a data network of the manufacturer, to improve the devices and capitalize on the data. P10 did draw a circular connection of the internal devices with a gateway router to the external network, mentioning WLAN as the commmunication devices, P14 did only mention an internal storage and interconnected the devices, but did not mention any other devices, that are neccessary for the system to achieve the connectivity. When ignoring the external focus, P10's drawing would be categorized as a basic model, P14's as a limited model.

4.1.4 Lack of Knowledge

Apart from different dataflow mental models, participants' lack of knowledge or misinformation towards certain smart devices leads to a misguided perspective towards certain areas of the smart home.

Smart Home Devices. Some participants had a limited understanding of the capabilities of smart home devices. Participants were asked to try and explain the dataflow of certain scenarios (appendix A1) like externally switching of the lights in the smarthome, after being notified of lights still being switched on, which was not always comprehensible to all participants :

> *"I also do not know who registers that I am out of the house and what registers that I am out of the house and what registers that the lights are still on, no idea."* (P13)

Other participants questioned the purpose of devices, as some seemingly replace old technology, while not really offering something new. P12 noted, that he does not think most of the devices are smart. He continues to describe a scenario, that he would consider smart :

> *"It would be smart if it were to realize, hey it's raining today, [...] it's dark earlier, which means [the smart lights] have to start earlier, I could see that as smart."* (P12)

However ambient light sensors, are already built in laptops and phones, are able to track brightness and can also be implemented in a smart home to offer cited scenario [21].

Participants were not sure of data exchange between servers and smart home devices. It is not clear wheter all devices send their data to the manufacturer. When questioned where the data of a smart vacuum is saved and collected, participants mentioned the possibility, of the data being saved in the device itself. P7 mentioned :

> *"I think the robot has its own processing power, it does not need a cloud."*

Communication and Data transfer. As elaborated (in section 2.1), the SHS and the network of Internet of Things in general use a broad selection of communication protocols, all delivering a service for different circumstances. Most of the participants mentioned protocols like Bluetooth, Wifi (or more broadly WLAN), with single participants also mentioning ZigBee (P6) and Cellular (P7). However for some participants, the communication and data exchange of devices was not fully understood:

> *"I think if it works via Bluetooth or something like that, then I do not think there is a server where it is storaged."* (P2)

Bluetooth is a close range communication protocol, which only allows data transfers, when the devices are in close proximity of each other. However, this does not mean, that the data will not be send to the server after all. The SHS translates different protocols with gateways, which allows all data to traverse the network, that includes the transfer to servers. P5 distinguished between a connection via the Internet and an application. The distinction is between different interactions, some of them do need the Internet and simple interactions do not :

> *"I think in itself it is also a simple connection, because only mechanically something goes up and down. Compared to the others, it is not a connection to the Internet in the sense that it is now looking for something special."* (P5)

This perspective implies, that only more complex interactions will send data to the Internet (the participant probably refers to the Internet as a synonym to servers of the manufacturer, where data is processed), while simple ones do not. P9 described a similiar situation, in which data transfer does not include any companies, as a mechanical interaction does not send the data to external entities :

> *"It is controlled by the sensor in the end and here with the blinds in the same way. I can start a sensor because I have a motor here and when the motor is activated, nothing additionally happens. This means that other companies are not involved in any way [...]."*

Many devices of the smart home do not require external processing power, in order to accomplish their goals, however status updates and acknowledgments are shared with the system in order to have an accurate representation of the situations in the smart home and therefore can include data transfers to external companies. Only one of the participants mentioned potential data tapping when the data is send via communication protocols :

> *"Until it gets to the server, it will probably go one way where the data can be hacked, but that would probably be the WLAN or other Internet connections."*

Communication protocols can be the subject of adversaries. Especially within the WSN and the local network, as sensors and actuators have none or limited storage capacity, forcing the security of the data transfer to be small in size. This could allow intruders to breach the system and modify or intercept the dataflow [2]. Many participants underestimated the capabilities of smart home interoperability and questioned the purpose of certain devices, as some interactions were thought to not be possible yet.

4.2 Interview Themes

The analysis of the interviews has lead to four main topics. First, participants are concerned with the use and collection of their personal data. Sensitive data is recorded and leaves the home, creating a threat for the user privacy. Second, current vulnerabilities of technology raise concerns towards security. The third topic revolves around the trust of participants towards the companies collecting the data of the users and how it affects privacy and smart home investment. At last, participants also question the purpose and current functions of the smart home. Rather than enhancing life, some do not see a real benefit of the current devices.

4.2.1 User Concerns toward Data Collection and Use

All participants in the study raised concerns regarding the creation, transfer and collection of data in the smart home. Participants were particularly concerned with the data transfer that leaves the smart home and goes to the manufacturer. Some have no idea what data is collected, which part leaves the home and what happens with it. Some figured, the data is either processed by algorithms to figure out tasks or it is collected for other purposes like device updates, selling the data and creating a data profile of the user:

> *"Nowadays it works in such a way that you, as a layman, simply plug it in everywhere and you are happy: "I can watch TV, I can go on the Internet", but you don't know what data from the TV will flow back to the manufacturer."* (P15)

Next to financial reasons, participants with no smart home devices named data concerns as a reason for why they have not yet invested in the technology:

> *"First, I'm scared because I don't know exactly what's going to happen with the data [...]"* (P14)

P11 and P12 marked specific spots in their drawing, asking specific question about the data use of the company :

> *"Information about this (points to the data flow to and from the server) is always very bad. How this data is recorded, whether only connection data is stored for a certain time or whether content is stored, whether this is encryption that I can influence [...]"* (P12)

Participants also raise concerns with devices, for which the connection to the Internet does not seem neccessary:

> *"According to my understanding, the chips that are available today are so powerful, that it [smart vacuum] would not need any additional information at all... it can store everything... nobody can tell me that I need an Internet server for this somewhere."* (P12)

> *"Actually, the data would not need a cloud anywhere. All it [Smart Vacuum] would have to have would be a big chip. [...] It's just ridiculous what [little] amount of data there is."* (P11)

Most participants are generally concerned, without being specific. Generally, they are concerned about private data. Many generally believed that all data is more or less sensitive. Some specifics that are mentioned, include concerns towards collected data that will be used against them, like political, religious or other views, that might not be tolerated. P7 just generally despises the idea of being monitored and P10 is very critical of personalized advertisement. One commonly raised argument, that came up when talking about scenario two (see A.1) was the insurance company, which could exploit health data in order to raise the monthly payment:

> *"Through your eating habits, one can also find out if you are rather obese and maybe the data will be resold to some pharmacy company [...] or maybe to insurance companies [...]"* (P10)

> *"A conclusion [...] via the health data, for example, that I have a liver cerosis somewhere and this in turn is also reported to my health insurer, who then gives me a corresponding premium."* (P9)

4.2.2 Security and Reliability Concerns

While the most participants were only concerned with their data, a few particpants raised specific security concerns, as well as concerns towards reliability of the system. The fear of P10, P11, P14 was especially directed towards unauthorized people, who gain access to the user's SHS and extract sensitive data:

> *"Or what if somebody hacks it? And then somehow unlocks it on their own."* (P14)

While the fear of hackers was raised, no specifics were given. Participants did not further explain the goal of adversaries, which attacks could be possible and what data is particularly in danger. Another concern is the fact, that these devices are reliant on an Internet connection. Replacing other devices, could create a dependency on Internet availability:

> *"I have the feeling that the systems are relatively vulnerable and therefore the benefit is suddenly plagued by an overwhelming failure rate and then the price and the effort to think about it is sometimes not worth it."* (P11)

P7 reports about an anecdote, that happened to relatives with a smart door lock, which opened the front door at night, due to a proximity indication of a phone from the inside triggering the lock, after it recharged:

> *" My father had the case [...] that my stepsister came home at night with her boyfriend [...] her mobile phone [was] empty, she plugged it in, at night it turned on and the door opened [...]."* (P7)

Due to the specific selection of participants with little to no smart home experiences, the overall concern towards security were scarce and very general. Participants did mention the general threats, they already face with an Internet network and were more focused on the threats towards privacy. When asked about it, participants named security as a main reason to purchase a smart home, which could generally indicate, that security features are believed to be more reliable, compared to the overflow of privacy concerns.

4.2.3 User's Benefits Perception

The smart home functionality and benefits of today were perceived with mixed feelings. While some of the participants valued current products for their functionality, many of the participants criticized devices for only providing convenience, which is partially seen as unneccessary, takes the control out of the hands of the user and leads to lazyness:

> *"I work for a coffee machine manufacturer [...], our coffee machines are connectable to WLAN and I can use an app to select a coffee and start it, but the machines already have a touchdisplay where I can do all these functions, so why do I just not do it on the machine, rather than with the phone, in front of my machine?"* (P12)

> *"So for me, a disadvantage of the Smart Home is that I want to control what's going on myself, I do not want to be dependent on such a device [...]".*(P2)

> *"[...] secondly, I also notice, that it creates an insane amount of laziness [...]"* (P14)

Technically affine participants called for interoperability between the devices, to simplify the installation and allow for more control :

> *"As long as you have to use some type of a bridge yourself - buy something else separately, it's always a bit of an obstacle and I think that's more of a problem."*(P1)

> *"I already had the idea to install a Smart Home at home and at some point I said "No". If I need an extra part for this and I need an extra part for that and I need an extra part for this as well, then that's just too silly for me."* (P15)

The participants with less technical interest, asked for quick and easy ways to install the devices or teach them about the smart home system and how to use it :

> *"[...] and it should also be explained how to use them [the devices]. Maybe on courses or seminars or simple video clips, how to use it."* (P5)

> *"So I think if I had a simple system and could get simple advice and so on and everything from one source, I would definitely be interested."* (P8)

> *"Someone who sells something like that would have to immediately offer to teach people, what they are actually using."* (P9)

Against the results of related research, only one participant was clearly willing to share his data, if he receives more comfort from the devices.

> *"Yes - well, I would be willing to give more data for this, if I have more comfort for it - because I think that both are connected. The device can only offer comfort if it has enough information."* (P5)

This does not mean however, that others are not eventually giving away their data as well. Most participants emphasized to be very much against the trade-off. A recurring theme from privacy concerned participants was the data exploitation of consumers. Companies are using new technology to lure in consumers and despite of the users being concerned with their data, the technology makes the trade-off worth it to them, as they are not aware of the repercussions. P11 states that one has no choice but to conform with the current procedures, if one tries to keep up with the world :

> *" You have to live on the internet and you can't get anything on the internet without disclosing your data, because some people have figured out that the fastest way to spread, is when a fair service is not compensated with a fair payment, but rather let him [user] believe that he gets it for free and then virtually seduce him."* (P11)

As most valuable benefits of the smart home, the participants mentioned health, security and energy as well as the general concept of making life easier. Health benefits were seen especially positive for elderly or disabled people. Security was mentioned as a useful implementation, when you have multiple residences:

> *"My father had a few accommodations in different places on the planet where he was staying and [...], there was always burglaries at the places he was not present and I always thought it would be nice to have the camera always standing there [...]* (P11)

5 Design Recommendations

Next to the concerns, that were raised during the interview, participants expressed values and ideas, they would like to see implemented in the future smart home.

5.1 Transparency and Security

The most frequent keyword used by the participants was “transparency”. The majority of participants underlined the importance to know, what happens with the data :

> *“So I guess why so many people do not use it yet - On the one hand transparency, what happens with data, that is one of the most important and sensitive things[...]”* (P1)

> *“Somehow it would have to be guaranteed that my privacy is secured and there would have to be complete transparency about the data.”* (P4)

> *“So I would work on the first point, how do you really handle the data, that you try to make the transparency, that you just make a healthy and reasonable privacy. I think that’s the be-all and end-all to reinforce people’s belief in the smart home.”* (P14)

> *“First of all the security of your data, that you can make sure that the data really just stays where it belongs, unless you give a certain permission where you say the data can be given away for further development of the technology.”* (P15)

Some of the participants explicitly mentioned, that the data collection would be okay, if the use of the data could be comprehensible and made sense or if the data was processed anonymously :

> *“The question for me is always, what does the recipient need the data for? If it makes sense for me, if I know they somehow need the brightness in my room to make my display brighter or darker, that makes sense for me. Why does the flashlight need my location, that’s something different, that’s what I think it’s more about.”* (P2)

P8 is specificly concerned with the security and identification of the data. If these specifics are assured, data collection could be acceptable:

> *“Of course, the data can perhaps also be evaluated in order to improve the devices - one would not be so much against that. So there would have to be a certain security that the data is anonymous [...].”* (P8)

Next to the general transparency regarding data, two participants mentioned transparency of connectivity. The idea is to give the user an indication, when data is sent to external entities or what data is being used currently :

> *“It would be so cool, if you could give the customer an interface, if you buy such a device and the customer can then really set it up himself, giving information to the data he passes on - what happens with the data, really providing information to it - that would already help a lot.”* (P10)

> *“I think that many people would be quite worried if devices in the house that see me, such as the TV, had a lamp on all the time” - Just as the lamp indicates that it [the TV] is on [...] - why is there not something for the Internet? Why does it not tell us “You’re on the Internet right now” and the device synchronizes continuously - people would go crazy and start questioning their data usage and data disclosure [...].”* (P7)

P12 encourages companies to work in collaboration with consumers and let them take part in the development of the device, to create trust and transparency at the same time:

> *"My idea to the companies, make the products open [source], deal openly with what you do with the data [...] create transparency and thus you also get customers who give back, who also reward you for it [...]."* (P12)

5.2 Reduced External Data Flow

Some participants would rather see structural change regarding the data communication, than relying on data transparency. At best, the system would be self-contained. While related papers did not see this as a possible option [86], since core features like remote control are seen as a crucial feature [83], some participants prefer that trade-off:

> *"The best thing would be to have your own server, where your data [...] is stored, without the data leaking out, without anyone being able to infer consumer behaviour from it [...]. Only if you then agree correspondingly, the data may also be used."* (P15)

> *"What I actually think about are light bulbs, but I don't need light bulbs that I have to switch off from outside the house, I just need a light bulb where I don't have to get up from bed"* (P12)

5.3 Standardization

Participants who own smart devices or thought about purchasing smart devices, criticised the industry for not having a standard, that can bring together smart home devices in a quick and easy manner :

> *"Simply that it is open for everything, that I can easily combine the services with each other, so that everything is somehow connected on If This Than That, just [have] open interfaces and that [the network] can communicate smoothly with each other."* (P6)

Not only do more devices offer an increase of possible threats, as each individual node within the system needs their own protective measures, but also the time consumption and the neccessary knowledge regarding creating a fluent communication between the devices requires time investment of the user.

6 Discussion

The results of the interviews continue to shape a group of themes, following the trend of prior research revolving around user perception of smart homes. The core topics, that have come out of the study will now be discussed and reflected upon.

6.1 Sufficient Models

Despite of focusing on mostly non smart home users, the data flow models of the participants were comparable to actual smart home adopters. Similiar to related work in the same field, participants showed varying degress of roughly the same base concept of devices being connected with each other, controlled by one main device, with some gateway device connecting the internal network with the external one, where the manufacturer is analyzing data, improving the device and sending it back to the user. We identified three different mental models, a limited model, a basic model and a critical one. Basicially the main difference of the models was defined by the fidelity of of either the internal or the external model. The limited model had a vague understanding of internal and external data flow, with the basic model showing the key nodes of the internal network. It generally shows all important entities of the system. The critical model paints a broader picture with second order data exchange between manufacturers and potential third party companies. In the last decades, the Internet has become an integral part of life and while technical knowledge still differs between consumers, the base perspective is very much built upon the same understanding. Server, router, bluetooth and WLAN have become basic words in the daily routine of society and while the technology might improve and develop, the core ideas of connected devices stay roughly the same. The biggest lack of knowlegde lies in the sequence of communication, how communication protocols differ from each other, when data needs to leave the smart home and also when it connects with the Internet even though it does not execute a direct service. Participants are not always capable to figure out how certain devices figure out conditions, however they do know, that collecting lots of personal data of any sort can be telling a lot about the user.

6.2 Overwhelming Privacy Concerns

Without hesitation, participants shared their privacy concerns. Against the odds of related works in the field, interviews were driven by this topic. For non-users, privacy concerns are the main reason for holding back on smart home devices. Particularly the lack of knowledge regarding the dataflow happening outside was the key talking point of the interviews. The general idea of collecting data, is not primarily the problem, but rather the questions that come along with it. Participants want to know what particular data is collected from which device, why the data must be collected, what is analyzed and when exactly devices send data out to the Internet. Some mentioned the importance of the final control and approval of the data by the user. Next to clarity about data collection, it also needs to be anonymous and should not be retraceable. While many did accept the privacy trade-off by buying devices, that collect data in one way or another, different to other studies, where users accepted the deal, participants reacted with ongoing displeasure even months after the purchase, even unplugging the device. Data within the smart home is generally seen as sensitive data, that needs to be secure and protected.

6.3 Mixed Feelings regarding Benefits

The core functionality of smart homes is understood to currently build around the goal of comfort and remote controlling devices of the smart home. While the concept and main functions of most devices are understood, participants believe that the devices do not improve the quality of life to a considerable degree. The understanding of the devices is mostly one dimensional, with the

considered functionality not or barely taking into account the network of devices, that could potentially create a sequence of automations. Some features also take away work aspects of life, that some participants consider to be important and would like to carry on. Going to the supermarket, cleaning the house and figuring out things without being reliant on the technology are values, that some of the participants expressed. Benefits of some devices were not considered to be useful. Requesting data queries and setting reminders was not enough to justify the constant collection of data. Replacing certain devices like a coffee machine, that already has a quick and easy interface did not seem useful. The core benefits, people are expecting to receive with a smart home are security, health, energy reduction and gaining more free time. Due to the lack of standardization, the required knowledge to set up the system and the constant attention towards technology, people believe that these devices generally require more time to figure out than they are saving.

6.4 Learned Helplessness - The Trust Paradox

One of the interview questions explored wheter or not the comfort of devices can influence the user to grant access to data, that was previously rated as sensitive. Some participants believed it to be a trade-off that the user has to "pay" in order to gain the benefits of the devices. Others criticised the trade-off and showed discomfort. The comfort of people and the invisible collection of data, combined with long and complex terms of services seduce people to unconciously approve a trade-off, that is unwillingly approved. While this situation is described as the trust paradox [36], related papers simply identify it as such, without questioning the problem. Participants describe the trade-off as a "trick" (P10), a form of "seduction" (P11) and generally show a helplessness, that is either accepted or leads to total rejection of the technology (P13).

6.5 Adapting the System with Help

Participants with the lowest ATI score, expressed the need for guidance. The complexity of the system without active help from the manufacturer makes it hard for the people to get involved. Participants would have aquired devices already, if companies assure them with support and potential tutorial videos or courses to get familiar with the possibilities of the system.

6.6 Standardization

Next to the need for help, some participants ask for a more standardized system, where devices are able to collaborate without an extensive installation process.

7 Conclusion and Future Work

In this final section, the conclusion to this thesis is presented and recommendations for future research are suggested.

7.1 Conclusions

This thesis was about understanding the smart home mental models of potential users, including additional concerns of the user. These models will help build an environment, that allows users to make a well informed decision regarding the extensive data collection of smart home devices. Early research regarding ubiquitous computing [42] has already pointed out 19 years ago, that the data collection of smart devices will be limitless and create tension and discomfort between users and the manufacturers.

The conducted study has collected a clear opinion of the users, that does align with core results of related papers, while the severity and importance of preserving the privacy was clearly present, in comparison to research conducted in other countries. The key points of this problematic relation remains on the side of the manufacturer. The results of this study show, that the lack of knowledge regarding data collection and storage practices results in distrust towards the manufacturer. Despite interest, the participants reject the smart home because they are afraid for the security of their personal data. While smart home adopters mostly accept the trade-off, they also desire answers regarding what, why and when data is leaving the home network. Some do clearly state, that the collection of data is not neccessarily the problem, if the purpose for it is clear and retraceable. For non-users, the smart home benefits are currently not enough, to justify giving up on the data. Benefits of the most popular devices are heavily leaning towards comfort, which some particiants do not desire. Participants see meaningful benefits in areas like energy, health and security, though these products are not as apparent in the media. Next to privacy, participants did also raise concerns, towards the standardization of smart home technology. The constraint of having to buy multiple bridges to allow communication between devices is creating a time consuming process that participants are not willing to buy into. Participants with lack of technical knowledge call for more support and campaigns, that help them join the discussion.

7.2 Future Work

The study further underlined the main problem of the current privacy discussion in smart home and ubiquitous computing literature in general. It is hard to say, how much the manufacturers can be influenced, as smart home adopters do accept the trade-off, despite asking for more transparency. The goal of future designs should be concerned with the best possible implementation of transparency. The question remains, how much information about data communication the users want. Potential work could go towards building prototypes of interfaces, that provide the user with privacy data, that is easy to understand, yet delivers enough information regarding data use. The key questions are “What data is collected?”, “Who gets the data”, “Why is it collected?”, additionally it should further be researched, how users would feel about an indication, when the data is leaving the home network.

Another direction is to counter privacy flaws with additional devices. As participants already show frustration towards the neccessity of multiple devices, this should be recognized as an undesireable alternative, as counter measures would have to be adapted to several devices and could always require new solutions for new devices. However, it makes sense to develop privacy protective devices for popular devices. Some work has already started in this direction e.g. Gao et al. have proposed a framework preventing smart assistants to constantly listen, jamming the audio

recording till the user is close enough and executes a real voice command [28]. In any way, research needs to not only prevent data leaving the network, but also deliver detailed, yet easy information about data collection and find ways, how to deliver it to the user.

Content of the enclosed CD

1. Electronic version of the thesis in original format and PDF.
2. Data collected in the course of the Study (Audio and Video via USB-stick).
3. All available cited sources in electronic form.

References

[1] William Ablondi. *2018 Global Smart Home Forecast*. accessed December 24, 2019. URL: https://www.strategyanalytics.com/access-services/devices/connected-home/smart-home/market-data/report-detail/2018-global-smart-home-forecast#.WwWtm-4vyUk%20IndustryARC.

[2] Ahlam Alami, Laila Benhlima, and Slimane Bah. "A Study of Security Requirements in Wireless Sensor Networks for Smart Home Healthcare Systems". In: *Proceedings of the 3rd International Conference on Smart City Applications*. ACM. 2018, p. 55.

[3] Frances K Aldrich. "Smart homes: past, present and future". In: *Inside the smart home*. Springer, 2003, pp. 17–39.

[4] Maggie Astor. *Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared*. New York Times. accessed January 9, 2020. 2017. URL: https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html.

[5] Sheikh Izzal Azid and Sushil Kumar. "Analysis and performance of a low cost SMS based home security system". In: *International Journal of Smart Home* 5.3 (2011), pp. 15–24.

[6] Christopher W Badenhop et al. "The Z-Wave routing protocol and its security implications". In: *Computers & Security* 68 (2017), pp. 112–129.

[7] Hyun Jae Baek et al. "A smart health monitoring chair for nonintrusive measurement of biological signals". In: *IEEE transactions on Information Technology in Biomedicine* 16.1 (2011), pp. 150–158.

[8] Jayashri Bangali and Arvind Shaligram. "Design and Implementation of Security Systems for Smart Home based on GSM technology". In: *International Journal of Smart Home* 7.6 (2013), pp. 201–208.

[9] Peter A Bibby and Stephen J Payne. "Instruction and practice in learning to use a device". In: *Cognitive Science* 20.4 (1996), pp. 539–578.

[10] Ilse Bierhoff et al. "Smart home environment". In: *Towards an inclusive future–Impact and wider potential of information and communication technologies. East Sussex Press, Brussels, Belgium* (2007).

[11] Virginia Braun and Victoria Clarke. "Thematic analysis." In: (2012).

[12] Marie Chan, Eric Campo, and Daniel Estève. "Assessment of activity of elderly people using a home monitoring system". In: *International Journal of Rehabilitation Research* 28.1 (2005), pp. 69–76.

[13] Marie Chan et al. "A review of smart homes: Present state and future challenges". In: *Computer methods and programs in biomedicine* 91.1 (2008), pp. 55–81.

[14] J Chandramohan et al. "Intelligent smart home automation and security system using Arduino and Wi-fi". In: *International Journal of Engineering And Computer Science (IJECS)* 6.3 (2017), pp. 20694–20698.

[15] Liang Chen, Suiming Guo, and Guoqiang Zhang. "Distributing very-large content from cloud to smart home hubs: Measurement and implications". In: *2015 IEEE International Conference on Communications (ICC)*. IEEE. 2015, pp. 364–369.

[16] Meghan Clark, Mark W Newman, and Prabal Dutta. "Devices and data and agents, oh my: How smart home abstractions prime end-user mental models". In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1.3 (2017), p. 44.

[17] Diane J Cook et al. "MavHome: An agent-based smart home". In: *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003.(PerCom 2003)*. IEEE. 2003, pp. 521–524.

[18] James L Crowley and Joelle Coutaz. “An ecological view of smart home technologies”. In: *European Conference on Ambient Intelligence*. Springer. 2015, pp. 1–16.

[19] Mohsen Darianian and Martin Peter Michael. “Smart home mobile RFID-based Internet-of-Things systems and services”. In: *2008 International conference on advanced computer theory and engineering*. IEEE. 2008, pp. 116–120.

[20] M Jamal Deen. “Information and communications technologies for elderly ubiquitous healthcare in a smart home”. In: *Personal and Ubiquitous Computing* 19.3-4 (2015), pp. 573–599.

[21] Declan T Delaney, Gregory MP O’Hare, and Antonio G Ruzzelli. “Evaluation of energy-efficiency in lighting systems using sensor networks”. In: *Proceedings of the First ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings*. ACM. 2009, pp. 61–66.

[22] Melike Erol-Kantarci and Hussein T Mouftah. “Wireless sensor networks for cost-efficient residential energy management in the smart grid”. In: *IEEE Transactions on Smart Grid* 2.2 (2011), pp. 314–325.

[23] Harry Fairhead. *There Really Are No More IPv4 Addresses*. accessed January 13th, 2020. Oct. 2019. URL: https://www.i-programmer.info/news/81-web-general/13210-there-really-are-no-more-ipv4-addresses.html.

[24] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. “Security analysis of emerging smart home applications”. In: *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2016, pp. 636–654.

[25] Behrang Fouladi and Sahand Ghanoun. “Honey, i’m home!!, hacking zwave home automation systems”. In: *Black Hat USA* (2013).

[26] Lorenzo Franceschi Bicchierai. *How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet*. Vice. 2016. URL: https://www.vice.com/en_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs.

[27] Thomas Franke, Christiane Attig, and Daniel Wessel. “Assessing Affinity for Technology Interaction - The Affinity for Technology Interaction (ATI) Scale.” In: *Unpublished manuscript.* (2017).

[28] Chuhan Gao et al. “Traversing the Quagmire that is Privacy in your Smart Home”. In: *In Proceedings of the 2018 Workshop on IoT Security and Privacy (pp. 22-28). ACM.* (2018).

[29] Kevin Ghirardello et al. “Cyber security of smart homes: Development of a reference architecture for attack surface analysis”. In: *Future Internet* (2018).

[30] Khusvinder Gill et al. “A zigbee-based home automation system”. In: *IEEE Transactions on consumer Electronics* 55.2 (2009), pp. 422–430.

[31] Splendid Research GmbH. *Smart Home Monitor 2019*. accessed January 2nd, 2020. URL: https://www.splendid-research.com/de/smarthome.html.

[32] Jayavardhana Gubbi et al. “Internet of Things (IoT): A vision, architectural elements, and future directions”. In: *Future generation computer systems* 29.7 (2013), pp. 1645–1660.

[33] Jaap C Haartsen. “Bluetooth radio system”. In: *Wiley Encyclopedia of Telecommunications* (2003).

[34] IndustryARC. *Smart Homes Market - Forecast(2020 - 2025)*. accessed January 8, 2020. 2019.

[35] Tarikul Islam, Subhas Chandra Mukhopadhyay, and Nagender Kumar Suryadevara. “Smart sensors and internet of things: a postgraduate paper”. In: *IEEE Sensors Journal* 17.3 (2016), pp. 577–584.

[36] Harvey S James Jr. “The trust paradox: a survey of economic inquiries into the nature of trust and trustworthiness”. In: *Journal of Economic Behavior & Organization* 47.3 (2002), pp. 291–307.

[37] Arun Cyril Jose and Reza Malekian. “Smart home automation security: a literature review”. In: *SmartCR* 5.4 (2015), pp. 269–285.

[38] Ruogu Kang et al. ““My Data Just Goes Everywhere:” User Mental Models of the Internet and Implications for Privacy and Security”. In: *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*. 2015, pp. 39–52.

[39] Georgios Kavallieratos et al. “Threat Analysis for Smart Homes”. In: *Future Internet* 11.10 (2019), p. 207.

[40] Patrick Kinney et al. “Zigbee technology: Wireless control that simply works”. In: *Communications design conference*. Vol. 2. 2003, pp. 1–7.

[41] Predrag Klasnja et al. “When i am on wi-fi, i am fearless: privacy concerns & practices in eeryday wi-fi use”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM. 2009, pp. 1993–2002.

[42] Marc Langheinrich. “Privacy by design—principles of privacy-aware ubiquitous systems.” In: *International conference on Ubiquitous Computing* (2001).

[43] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. “Alexa, are you listening?: Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers”. In: *Proceedings of the ACM on Human-Computer Interaction* 2.CSCW (2018), p. 102.

[44] Reuel O. Launey et al. *Expandable home automation system*. US Patent 5,086,385. 1992.

[45] Gilles LeBellego et al. “A model for the measurement of patient activity in a hospital suite”. In: *IEEE Transactions on information technology in biomedicine* 10.1 (2006), pp. 92–99.

[46] Hui Liu et al. “Smart solution, poor protection: An empirical study of security and privacy issues in developing and deploying smart home devices”. In: *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*. ACM. 2017, pp. 13–18.

[47] Natasha Lomas. *Critical flaw identified in zigbee smart home devices*. 2015.

[48] Lucintel. *Smart Homes Market Report: Trends, Forecast and Competitive Analysis*. accessed January 9, 2020. 2019. URL: https://www.reportlinker.com/p05817488/Smart-Homes-Market-Report-Trends-Forecast-and-Competitive-Analysis.html?utm_source=PRN.

[49] Sumit Majumder, Tapas Mondal, and M Jamal Deen. “Wearable sensors for remote health monitoring”. In: *Sensors* 17.1 (2017), p. 130.

[50] Naresh K Malhotra, Sung S Kim, and James Agarwal. “Internet users’ information privacy concerns (IUIPC): The construct, the scale, and a causal model”. In: *Information systems research* 15.4 (2004), pp. 336–355.

[51] Davit Marikyan, Savvas Papagiannidis, and Eleftherios Alamanos. “A systematic review of the smart home literature: A user perspective”. In: *Technological Forecasting and Social Change* 138 (2019), pp. 139–154.

[52] Yasushi Masuda et al. “An unconstrained monitoring system for home rehabilitation”. In: *IEEE engineering in medicine and biology magazine* 24.4 (2005), pp. 43–47.

[53] Armbrust Michael et al. “A view of cloud computing”. In: *Communications of the ACM* 53.4 (2010), pp. 50–58.

[54] Alex Mihailidis, Brent Carmichael, and Jennifer Boger. “The use of computer vision in an intelligent environment to support aging-in-place, safety, and independence in the home”. In: *IEEE Transactions on information technology in biomedicine* 8.3 (2004), pp. 238–247.

[55] Pardis Emami Naeini et al. “Privacy expectations and preferences in an IoT world”. In: *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*. 2017, pp. 399–412.

[56] Dusit Niyato, Xiao Lu, and Ping Wang. “Machine-to-machine communications for home energy management system in smart grid”. In: (2011).

[57] Patricia A Norberg, Daniel R Horne, and David A Horne. “The privacy paradox: Personal information disclosure intentions versus behaviors”. In: *Journal of consumer affairs* 41.1 (2007), pp. 100–126.

[58] Sukhvir Notra et al. “An experimental study of security and privacy risks with emerging household appliances”. In: *2014 IEEE Conference on Communications and Network Security*. IEEE. 2014, pp. 79–84.

[59] Kirsten KB Peetoom et al. “Literature review on monitoring technologies and their outcomes in independently living elderly people”. In: *Disability and Rehabilitation: Assistive Technology* 10.4 (2015), pp. 271–294.

[60] Sunil K. Rao and Raman K. Rao. *Home Automation And Smart Home Control Using Mobile Devices And Wireless Enabled Electrical Switches*. US Patent App. 14/100,975. 2014.

[61] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. “Why doesn’t Jane protect her privacy?” In: *International Symposium on Privacy Enhancing Technologies Symposium*. Springer. 2014, pp. 244–262.

[62] Vincent Ricquebourg et al. “The Smart Home Concept : our immediate future”. In: *IEEE international conference on e-learning in industrial electronics.* (2006).

[63] Rosslin John Robles and Tai-hoon Kim. “A review on security in smart home development”. In: *International Journal of Advanced Science and Technology* 15 (2010).

[64] Shadi Al-Sarawi et al. “Internet of Things (IoT) communication protocols”. In: *2017 8th International conference on information technology (ICIT)*. IEEE. 2017, pp. 685–690.

[65] Christine Satchell and Paul Dourish. “Beyond the user: use and non-use in HCI”. In: *Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group: Design: Open 24/7*. ACM. 2009, pp. 9–16.

[66] Martin Serror et al. “Towards in-network security for smart homes”. In: *Proceedings of the 13th International Conference on Availability, Reliability and Security*. ACM. 2018, p. 18.

[67] Roger Silverstone and Leslie Haddon. “Design and the domestication of information and communication technologies - Technical change and everyday life”. In: (1996).

[68] Sam Solaimani, Wally Keijzer-Broers, and Harry Bouwman. “What we do–and don’t–know about the Smart Home: an analysis of the Smart Home literature”. In: *Indoor and Built Environment* 24.3 (2015), pp. 370–383.

[69] Statista. *SMART HOME REPORT 2019*. accessed January 9, 2020. 2019. URL: https://www.statista.com/outlook/279/100/smart-home/worldwide.

[70] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. “" I don’t own the data": End User Perceptions of Smart Home Device Data Practices and Risks”. In: *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*. 2019.

[71] Sudeep Tanwar et al. “An advanced Internet of Thing based security alert system for smart home”. In: *2017 International Conference on Computer, Information and Telecommunication Systems (CITS)*. IEEE. 2017, pp. 25–29.

[72] Endel Tulving and Daniel L Schacter. “Priming and human memory systems”. In: *Science* 247.4940 (1990), pp. 301–306.

[73] Robert H Walden. “Analog-to-digital converter survey and analysis”. In: *IEEE Journal on selected areas in communications* 17.4 (1999), pp. 539–550.

[74] Samuel D Warren and Louis D Brandeis. “Right to privacy”. In: *Harv. L. Rev.* 4 (1890), p. 193.

[75] Rick Wash. “Folk models of home computer security”. In: *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM. 2010, p. 11.

[76] Mark Weiser. “The computer for the 21st century”. In: *ACM SIGMOBILE mobile computing and communications review* 3.3 (1999), pp. 3–11.

[77] Alan F Westin. “Privacy and freedom”. In: *Washington and Lee Law Review* 25.1 (1968), p. 166.

[78] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. “Smart homes and their users: a systematic analysis and key challenges”. In: *Personal and Ubiquitous Computing* 19.2 (2015), pp. 463–476.

[79] Davey Winder. *Confirmed: 2 Billion Records Exposed In Massive Smart Home Device Breach*. Forbes. accessed January 10, 2019. July 2019. URL: https://www.forbes.com/sites/daveywinder/2019/07/02/confirmed-2-billion-records-exposed-in-massive-smart-home-device-breach/.

[80] Peter Worthy, Ben Matthews, and Stephen Viller. “Trust me: doubts and concerns living with the Internet of Things”. In: *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*. ACM. 2016, pp. 427–434.

[81] Lu Yan et al. *The Internet of Things: from RFID to the next-generation pervasive networked systems*. Crc Press, 2008.

[82] Yaxing Yao et al. “Privacy Perceptions and Designs of Bystanders in Smart Homes”. In: *Proceedings of the ACM on Human-Computer Interaction* 3.CSCW (2019), pp. 1–24.

[83] Eric Zeng, Shrirang Mare, and Franziska Roesner. “End user security and privacy concerns with smart homes”. In: *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*. 2017, pp. 65–80.

[84] Serena Zheng et al. “User perceptions of smart home IoT privacy”. In: *Proceedings of the ACM on Human-Computer Interaction* 2.CSCW (2018), p. 200.

[85] Suyang Zhou et al. “Real-time energy control approach for smart home energy management system”. In: *Electric Power Components and Systems* 42.3-4 (2014), pp. 315–326.

[86] Verena Zimmermann et al. “‘Home, Smart Home’–Exploring End Users’ Mental Models of Smart Homes”. In: *Mensch und Computer 2018-Workshopband* (2018).

A Appendix

A.1 Interview Procedure

Drawing exercise

- Imagine you live in a fully functional "Smart Home". Sketch the system behind it considering the data flow. Besides the given devices, try to integrate all essential entities into the sketch. No entity in the data flow is taken for granted, it is better to draw more of the system than too little.

Questions regarding the drawing

- Please explain your sketch and train of thought.
- Attempt to explain, how the general data flows take place.
- Which devices in the system create data?
- Which devices in the system collect data?
- Choose an interaction of your system and try to describe the data flow of it.
- Where do you think the smart home's data is stored?

Base Questions - Smart Home

- What does the term "smart" mean? Can you name key features defining this term?
- When/how did you first learn about the term "Smart Home"?
- Have you ever interacted with a smart home (device) before? If so,which one?
- If you do not have a Smart Home yourself - is there a specific reason why?
- What are understandable reasons for you to invest / not to invest in a smart home ?

Data and Industry

- Is there specific data, that you give share without concern and is there data that you would never share?
- Do you think there is a relation between comfort and the sensitivity of data (Do people are more likely to give out sensitive data if they get more comfort in return?)
- Are there areas in the smart home system where the information should be more accessible and clear?
- If you had the opportunity to speak directly to the (smart home) industry, what points should they tackle in the future?
- What are understandable reasons for you to invest / not to invest in a smart home ?

Data Scenarios
In the following 3 scenarios you will have to think about the data flow again. Think about where the interaction starts and how the data flow through the system works. Name the positive and negative features of this particular scenario.

- A smart vacuum cleaner scans your apartment to be able to vacuum thoroughly and automatically in the future.
- A food item in the refrigerator was completely consumed - the Smart Fridge then reorders the product.
- A few lights of the house were not switched off and are now switched off externally with an app.

A.2 Summary of Participants' Demographics

Participant	Age	Sex	Employment	Field of Work	Living Situation	Own smart home device?
P1	25	M	Student	Web development	Living with my partner	No
P2	24	M	Student	Archaeology	Living with family	No
P3	28	M	Student	Human Medicine	Living with partner	Yes
P4	18	M	Student	IT	Living with family	No
P5	25	M	Student	German as foreign language	Living with family	No
P6	27	M	Academic worker	Education and Research	Living in a flat share	Yes
P7	23	M	Student	HCI	Living in a flat share	Yes
P8	64	F	Self-employed	Organisation	Living alone	No
P9	61	F	Self-employed	Real Estate Management	Living alone	No
P10	26	M	Student	Business Economics	Living with family	Yes
P11	59	M	Self-employed	Eventmanager	Living with partner	No
P12	37	M	(Self-)employed	IT-Administration	Living with partner	No
P13	32	F	student	Medicine	Living in a flat share	No
P14	37	M	employed	Event Planning	Living alone	No
P15	50	M	self-employed	Eventmanager	Living with Family	No

A.3 ATI Questionnaire

The ATI questionnaire works on the basis of a six point likert scale. It includes a total of 9-items :

i I like to occupy myself in greater detail with technical systems.

ii I like testing the functions of new technical systems

iii I predominantly deal with technical systems because I have to.

iv When I have a new technical system in front of me, I try it out intensively.

v I enjoy spending time becoming acquainted with a new technical system.

vi It is enough for me that a technical system works; I don't care how or why.

vii I try to understand how a technical system exactly works.

viii It is enough for me to know the basic functions of a technical system.

ix I try to make full use of the capabilities of a technical system.

Results of the survey :

Questions/ Participants	i	ii	iii	iv	v	vi	vii	viii	ix	Sum	Mean
P8	3	2	2	3	2	2	2	1	1	18	2,00
P13	2	2	3	2	2	2	4	3	3	23	2,56
P9	3	4	2	3	3	2	3	3	3	26	2,89
P5	2	4	6	4	4	1	2	3	5	31	3,44
P3	5	5	6	5	3	2	3	1	2	32	3,56
P2	4	5	4	5	5	2	3	3	2	33	3,67
P4	4	4	4	4	4	4	4	4	5	37	4,11
P14	5	5	4	3	4	5	4	4	5	39	4,33
P6	6	6	1	6	5	4	4	4	5	41	4,56
P11	5	5	4	5	5	5	5	4	4	42	4,67
P12	5	5	4	6	5	5	5	5	2	42	4,67
P15	5	5	2	5	4	6	5	5	5	42	4,67
P10	5	6	6	5	5	4	4	4	6	45	5,00
P7	6	6	5	6	5	5	4	4	5	46	5,11
P1	5	6	6	6	6	6	5	6	6	46	5,78

Figure A.1: ATI 9-Item Questionnaire

A.4 Internet Users' Information Privacy Concerns (IUIPC)

The IUIPC questionnaire works on the basis of a seven point likert scale. It includes a total of 10-items :

i Consumer online privacy is the consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.

ii Consumer control of personal information lies at the heart of consumer privacy.

iii I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.

iv Companies seeking information online should disclose the way the data are collected, processed, and used.

v A good consumer online privacy policy should have a clear and conspicuous disclosure.

vi It is very important to me that I am aware and knowledgeable about how my personal information will be used.

vii It usually bothers me when online companies ask me for personal information.

viii When online companies ask me for personal information, I sometimes think twice before providing it.

ix It bothers me to give personal information to so many online companies.

x I'm concerned that online companies are collecting too much personal information about me.

Question/ Participant	i	ii	iii	iv	v	vi	vii	viii	ix	x	M	SD
P1	7	6	6	7	7	5	4	5	4	4	5,5	1,2
P2	7	5	4	2	3	5	6	7	6	3	4,8	1,66
P3	7	6	6	6	7	3	3	7	3	3	5,1	1,48
P4	7	7	6	6	7	6	6	6	6	5	6,2	0,6
P5	6	7	7	6	7	6	4	6	6	6	6,1	0,83
P6	6	6	6	7	7	7	2	4	4	4	5,3	1,62
P7	6	6	7	5	6	7	3	4	5	7	5,6	1,28
P8	7	7	6	7	7	6	6	6	5	7	6,4	0,66
P9	5	6	6	6	6	7	5	6	6	6	5,9	0,54
P10	7	6	7	6	7	7	5	5	6	6	6,2	0,75
P11	7	6	6	7	7	7	5	5	5	7	6,2	0,87
P12	7	7	6	6	6	5	5	5	5	4	5,6	0,92
P13	6	7	7	7	7	7	7	7	7	7	6,9	0,3
P14	6	7	7	7	7	7	6	7	7	7	6,8	0,40
P15	6	6	2	6	6	6	6	7	7	7	5,9	1,37
M	6,47	6,33	5,93	6,07	6,47	6,07	4,87	5,80	5,47	5,53	5,9	0,97
SD	0,62	0,6	1,29	1,24	1,02	1,12	1,36	1,05	1,15	1,50	0,57	0,43

A.5 Data Sensivity Questionnaire

The data sensivity questionnaire includes 18-items, asking for the participants evaluation of the following data sets. The questionnaire is based upon a likert-scale with 4 points. The Possible answers are : 1.) not sensitive 2.) slightly sensitive 3.) sensitive 4.) very sensitive

i Contact-information (Name, Address, Zip-Code,...)

ii Sleeping patterns (movement in bed)

iii Status of the light sources at home

iv Movie-preferences

v Surveillance camera footage

vi Electricity-/water-/gas consumption

vii Fridge-inventary

viii Biometric data

ix Mobile photo album

x Voice recordings of a Smart assistant

xi Who is in what room in your apartment/house

xii How much you weigh

xiii How much you are exercising right now

xiv How much you have exercised historically

xv What time you will get home

xvi What your current heart rate is, and your historical heart rate trends.

xvii Whether you are currently calm, sleep deprived, focused, scatter-brained, anxious

xviii Whether a door or window in the apartment/house is open or closed

				How sensible is the following data for you?																
Question/ Participant	i	ii	iii	iv	v	vi	vii	viii	ix	x	xi	xii	xiii	xiv	xv	xvi	xvii	xviii	M	SD
1	2	2	0	1	3	1	1	2	3	1	1	2	1	1	1	1	3	3	1,61	0,89
2	2	3	3	3	3	2	3	2	3	2	3	1	2	2	3	2	2	2	2,39	0,59
3	1	2	0	0	3	0	0	3	3	3	1	1	1	1	2	2	2	2	1,50	1,07
4	3	0	1	0	3	2	1	2	3	2	1	1	2	2	1	1	1	2	1,56	0,90
5	2	0	0	0	0	0	0	0	3	3	3	0	0	0	3	0	3	3	1,11	1,41
6	0	3	2	0	3	1	1	3	3	2	1	1	2	1	1	2	2	1	1,61	0,95
7	3	0	0	0	3	2	1	3	3	3	2	1	1	1	1	2	2	3	1,72	1,10
8	1	1	2	1	3	1	2	3	3	2	3	1	2	2	2	2	3	3	2,06	0,78
9	1	3	2	3	3	1	2	1	3	2	2	2	2	1	1	1	3	1	1,89	0,81
10	1	2	0	1	3	2	1	3	3	3	3	3	3	3	3	3	3	3	2,39	0,95
11	1	2	2	1	3	2	2	3	3	2	3	2	2	2	3	2	3	3	2,28	0,65
12	1	2	2	3	3	2	3	3	3	3	3	2	2	2	2	3	2	2	2,39	0,59
13	1	3	2	2	3	2	2	3	3	2	2	1	1	1	2	1	2	1	1,89	0,74
14	1	3	3	2	3	2	2	3	2	3	3	2	2	3	3	3	3	3	2,56	0,60
15	3	0	0	1	3	0	0	2	2	2	3	3	3	3	3	3	3	3	2,06	1,22
M	1,53	1,73	1,27	1,13	2,80	1,33	1,40	2,40	2,87	2,33	2,27	1,53	1,73	1,67	2,07	1,87	2,47	2,33		
SD	0,88	1,18	1,12	1,18	0,75	0,79	0,95	0,88	0,34	0,60	0,85	0,81	0,77	0,87	0,85	0,88	0,62	0,79		

Figure A.2: Data Sensivity Questionnaire