LMU Munich
Frauenlobstraße 7a
D–80337 München
Institut für Informatik

Masterarbeit

Development of a Physical Smart Home Dashboard for Device Configuration and Privacy Awareness

Philipp Thalhammer

Course of Study:	Mensch-Computer-Interaktion
Examiner:	Prof. Dr. Sebastian Feger
Supervisor:	M.Sc. Maximiliane Windl

Commenced:	January 24, 2024
Completed:	July 24, 2024

“Development of a Physical Smart Home Dashboard for Device Configuration and Privacy Awareness”
July 24, 2024

Typesetting: PDF-LaTeX 2_ε

Kurzfassung

Über die letzten Jahre hat die Anzahl an Smart Home Geräten stark zugenommen. Zwar haben smarte Geräte viele Funktionen, die den Komfort von Nutzern erhöhen können, jedoch haben sie auch großen Einfluss auf Daten-Sicherheit und Privacy. Gerade in Shared-Spaces, wie beispielsweise in Haushalten mit mehreren Bewohnern, ist dies problematisch, da üblicherweise nur der Primärnutzer Zugang zu allen Informationen und Kontrollmechanismen von Smart Home Geräten hat. In dieser Arbeit stellen wir ein Smart Home Ökosystem vor, welches es allen Nutzern ermöglicht Einfluss auf die Daten-Sicherheit von einzelnen Smart Home Geräten zu nehmen. Das System beinhaltet ein tangible Dashboard, mit dessen Hilfe die Benutzer ihr Smart Home in der Form eines Grundrisses darstellen können, um Informationen über die Art und den Ort von smarten Geräten abzubilden. Um die Datenflüsse in Smart Homes transparenter zu gestalten, werden diese durch das Dashboard in Echtzeit visualisiert. Zusätzlich beinhaltet das Dashboard ein tangible Interface, um einzustellen ob das Gerät (1) nur innerhalb desselben Netzwerks verfügbar sein soll, (2) von überall durch einen verschlüsselten Service verfügbar ist oder (3) von überall verfügbar ist und auch durch Drittanbieter Geräte gesteuert werden kann. Wir haben eine "in-the-wild" Studie mit neun Teilnehmern in vier Haushalten über jeweils eine Woche durchgeführt. Dabei haben wir quantitative Daten über System-Logs und Fragebögen und qualitative Daten über semi-strukturierte Interviews gesammelt. Die Ergebnisse zeigen eine gute Usability des Dashboards und eine Erhöhung des Bewusstseins für Privacy. Wir konnten eine ausgeglichene Verteilung zwischen der Nutzung des digitalen und tangible Interfaces feststellen. Einige Nutzer gaben eine Präferenz für das digitale Interface, andere für das tangible Interface und wieder andere für eine Mischung aus beiden Modalitäten an. Auch wenn Privacy ein zweitrangiger Faktor für die meisten Nutzer ist, gibt es ein klares Bedürfnis nach besser zugänglichen Kontrollmechanismen. Gerade für Sekundärnutzer konnte unser System das Bewusstsein für Privacy erheblich erhöhen. Dies zeigt, dass zukünftige Systeme klare Kontrollmechanismen für Privacy beinhalten sollten. Um diese Kontrollmechanismen für eine möglichst große Menge an Nutzern zugänglich zu machen, sollten sowohl digitale als auch tangible Optionen angeboten werden.

Abstract

Over the last few years, the number of smart home devices has increased drastically. While smart devices bring a lot of convenience to users, they also introduce new privacy risks. This is especially problematic in shared spaces like households with multiple occupants, as usually, only the primary user gets access to privacy controls and information. We introduce a novel smart home eco-system that gives all users the ability to control their privacy for individual smart home devices. The system incorporates a tangible dashboard that lets users map out their smart home in the form of a floor plan to provide information about the type and location of smart home devices, while also visualizing data flow in real-time. Additionally, the dashboard features a tangible interface to control if the device should be accessible (1) only inside the same network, (2) from anywhere using an encrypted service, or (3) from anywhere and through third-party systems. We conducted an in-the-wild study with nine participants in four households for one week each and collected quantitative data through system logs and questionnaires as well as qualitative data through semi-structured interviews. Our results show that the dashboard was perceived to have good usability and is successful in raising users' privacy awareness. We found a balanced distribution in the use of tangible and digital privacy controls, with some users reporting a preference for digital controls, some for tangible controls, and others for a mixture of both. Although privacy is only a secondary priority for most smart home users, there is a clear demand for more accessible privacy controls. Especially for secondary users, our system improved privacy awareness significantly, suggesting the implementation of discrete privacy controls. Future smart home systems should incorporate both tangible and digital privacy controls, to make them accessible to a wider range of users.

Contents

List of Figures

1. Introduction

Over the last years connected devices and smart home appliances have gained massive popularity, with a predicted growth to 22 billion active Internet of Things (IoT) devices by 2025 [41], which even is on the more conservative side. These devices transform households into smart homes, defined as residences "equipped with computing and information technology which anticipates and responds to the needs of the occupants (...)" [6]. While the data that is collected by IoT devices might often appear irrelevant, in the hands of malicious actors it can become a serious threat. The work of Molina-Markham et al. [47] shows in great detail how much information can be gained simply from access to the data of a smart meter. This ranges from "how many people are in the home, sleeping routines, eating routines" [47] to even being able to tell if "there [is] a newborn in the house" [47] and can be deducted without prior training.

In shared spaces, the complexity of maintaining privacy increases due to the presence of different users and user types. While one might think of shared spaces as public places or office environments, even normal households can be considered 'shared'. These spaces can involve multiple occupants who might have different levels of awareness and concern about privacy risks as well as different access to privacy controls [5, 26]. As highlighted by Yao et al. [61], research about privacy and security often focuses on the primary user of the device and fails to account for other stakeholders like family members or visitors. The diversity of devices and the possibility of undisclosed IoT devices installed by others can create a challenging environment for ensuring privacy protection. Moreover, it is nearly impossible for users to track the data flow in smart homes, as devices usually lack any indication of this information.

The term 'Tangible Privacy' was introduced by Ahmad et al. [4] in 2020 as a way for users "to clearly and unambiguously control and discern privacy states of IoT devices in their vicinity" [4]. Since then the concept of using tangible interfaces to raise awareness about potential privacy risks in smart homes and shared spaces has been explored in greater detail. For instance, Delgado Rodriguez et al. [21] developed the '*PriKey*' tangible interface, which allows users to control the sensor capabilities *presence*, *audio* and *video* of all smart home devices in a room. Ahmad et al. [4] identified that understanding device states and their implications for functionality is a crucial need for users interacting with IoT devices. Building on this, Feger et al. [24] introduced '*ConnectivityControl*', which was later expanded in a model ecosystem by Thalhammer et al. [56]. '*ConnectivityControl*' extends the connectivity spectrum of IoT devices with a network-only mode and an access-point mode, in addition to the usual online mode [24]. This allows users to choose a state for each device, offering more granular control over the data flow in their smart home.

A survey of 1052 users conducted by Gerber et al. [27] found that the majority of participants were unable to identify real-world consequences associated with sharing their data through smart home and smart health devices. Even though some participants mentioned general privacy concerns like profiling and privacy violations, only a few were able to name specific consequences. Similar results were found in a survey over three countries in Europe, including Germany, by Kulyk et al. [35]. Tabassum et al. [54] found that participants recognized some threats and protective measures, but often perceived the privacy and security risks of their smart home devices as not important enough to change their behavior. This lack of awareness increases when users are in shared spaces instead of their own homes, because of the lack of information about what IoT devices are present and where they are located.

In his early work about privacy in persuasive computing Hong [29] posed a challenge: "let's make it so that when a person enters a room, he or she can reliably identify all of the sensors and data flows within 30 seconds." [29]. With inspiration from that, this thesis focuses on giving users discrete control over the way data flows inside a smart home system, while simultaneously offering real-time information about the

data flow. We present a tangible smart home dashboard, based on the work of Windl et al. [59], that lets users build a visual representation of their home in the form of a floor plan, including its IoT devices. The floor plan can be used by all stakeholders to easily identify the position and type of IoT devices in a home, while also empowering users to change the privacy state in a similar way to '*ConnectivityControl*' [24]. The dashboard has a grid with 16 rows and 16 columns of connectors, allowing for a total of 256 possible connections where 'proxy' devices can be plugged in. These proxies come equipped with a circular display and an incremental encoder that lets the user choose the privacy state of the device with the help of a simple user interface (UI). Through a set of three different Pins, with different voltages, the proxies can calculate their position on the dashboard, which is used to animate data flow between devices utilizing the dashboard's integrated LED matrix. The floor plan can be visualized using 3D printed plugs, to mark out the corners of a room and then be connected using colored string.

We conducted an in-the-wild study over four weeks, including a total of four households for seven to eight days each. Every household had two to three inhabitants and received (1) the tangible smart home dashboard and (2) the 'Privacy Hub' developed by Müller [48] to integrate the dashboard into a privacy-focused smart home eco-system. All participants were briefed on the purpose of the study and given instructions on how to use the system before the smart home components were installed. We collected demographic data, qualitative feedback as well as quantitative data for each participant.

Our results show that the system raised the privacy awareness of users and was able to make privacy controls accessible to all user types of a household. We found a significant increase in participants' perceived ability to protect their data within a smart home and to understand what happens with that data. The tangible component was perceived as fun and engaging, with participants using the tangible interface as frequently as the digital one. Although some users preferred the digital interface for convenience, we found strong support for tangible solutions or mixed approaches. Additionally, the dashboard was perceived to have good usability and was generally well-liked by the majority of participants.

This thesis will (1) provide information on related work about security and privacy in the context of smart homes, (2) describe the concept, build process, and functionality of the tangible dashboard prototype, and (3) present and discuss the results from a one-month long in-the-wild study with nine participants.

2. Related Work

2.1. Security and Privacy Vulnerabilities in Smart Homes

Smart home devices offer convenience and automation but also introduce a lot of security vulnerabilities that can potentially be exploited by malicious actors. These vulnerabilities stem from a range of different factors such as inadequate security protocols, lack of regular updates, and poor implementation. In the early work of Andrea et al. [10] about security and privacy vulnerabilities in smart homes, IoT security attacks are classified into four distinct categories: *Physical*, *Network*, *Software* and *Encryption* -attacks.

Physical Attacks require the attacker to have physical access to the device [10]. Physical attacks include, but are not limited to, *Physical Damage*, *Social Engineering*, or *Malicious Code Injection* [10].

Network Attacks are aimed at the IoT network and do not require the attacker to be physically near his target [10]. Network attacks include, but are not limited to, *Traffic Analysis Attacks*, *Sinkhole Attacks*, or *Man In the Middle Attacks* [10]. *Man In the Middle Attacks* are specifically interesting, as they are very common and "allow attackers to catch and manipulate communication between two end devices" [57], often without the user realizing that there was a security breach.

Software Attacks are the most common type of attack in computerized systems and revolve around the use of malicious software [10]. Software attacks include, but are not limited to, *Phishing Attacks*, *Virus, Worms, Trojan Horse, Spyware and Aware*, *Malicious Scripts*, or *Denial of Service* [10].

Encryption Attacks aim to break the encryption of an IoT system [10] and are perhaps the most interesting type of attack for this investigation, as they rely heavily on the poor security standards of IoT device manufacturers. Encryption attacks include, but are not limited to, *Side channel Attacks*, *Cryptanalysis Attacks*, or *Man In the Middle Attacks* [10].

Case studies highlight the impact of these vulnerabilities. For instance, in 2016, a major attack involved the Mirai botnet: the Mirai malware compromised numerous IoT devices, including IP cameras, printers, and routers, to launch a massive distributed denial-of-service (DDoS) attack, disrupting major internet services worldwide [11]. As of 2019, more than 100 million devices that feature Amazon's personal voice assistant, 'Alexa,' were sold [15]. In the same year, it was revealed that Amazon employees were listening to private conversations of their users to improve their service [14], showing that security and privacy threats not necessarily stem from outside attackers but can also be carried out by the manufacturers of the device itself.

As personal voice assistants are equipped with an always-on microphone [42], they pose a serious security risk. Additionally, they are often used as interfaces to smart environments [18], giving them access to data from other devices. The broader implications that personal voice assistants can have on privacy in smart homes were investigated in great detail by Lit et al. [40], highlighting the potential for attacks. Another crucial sensor type are smart cameras, as they are often installed in intimate places [39] and can record possibly sensitive video material. The type of data collected by smart homes varies with the number and type of active IoT devices. While some smart home appliances are equipped with high-sensitivity sensors (e.g., microphones and cameras), potentially giving intruders access to sensitive data, even presumably 'harmless' data can pose significant privacy risks in smart homes. The readings of an electricity smart meter, for example, are enough to tell how many people are home, routines like sleeping and eating, and even if there may be a newborn in the household [47]. Furthermore, it is possible to determine the location and type of IoT devices from data samples collected at the internet service provider (ISP) [51], which can provide insights

into the layout and functionality of a smart home network, further compromising privacy. The consequences of data breaches can range from companies selling user data for profit to more severe issues, such as concrete physical threats to the household's safety.

While standards for security and privacy in IoT systems do exist [32, 37], there is a lack of effective security standards specifically for smart environments like smart homes [32].

Smart home devices offer a lot of convenience and automation, but they also bring new threats to privacy and security. Case studies such as the Mirai botnet attack [11] and privacy scandals involving personal voice assistants [14] show the real-world consequences of these vulnerabilities. The diverse data that IoT devices collect can be used to extract sensitive information about smart home users [47, 51], even if it appears harmless at first. Even though standards for privacy and security exist [32, 37], research shows a lack of effective security standards for smart environments [32].

2.2. Privacy Awareness and User Perception

While users often value security and safety highly, privacy issues are overlooked [17]. This is caused by many different factors such as the complexity and inaccessibility of privacy information to users [50], the prioritization of immediate convenience and benefits brought by smart home devices [58, 63], and a lack of awareness about the extent of data collection practices [8, 42]. Users are often unable to name real-world consequences of privacy violations [27, 35], leading to a low prioritization of privacy. To develop a system that is capable of raising privacy awareness it is crucial to understand the factors that influence users' perception of privacy.

A key factor in this is the way that users are informed about privacy and security-related topics: privacy policies are often written in too complicated language [50], contain misleading information [50], or are simply presented in a way that users deem them not worth reading [49]. This suggests the use of a compact standardized label like proposed by Feger et al. [24], as McDonald et al. [45] also found out that "even the most readable policies are too difficult for most people to understand and even the best policies are confusing" [45]. The use of such standardized labels as a way to inform customers about privacy and security has been explored before and was found to be very effective [23]. Especially as users currently find it difficult to inform themselves about privacy and security implications before purchasing a device [23].

Some sources suggest that users tend to overlook the potential security risks that smart home devices may have and instead focus more on the benefits that they could bring [58]. However, others imply "that perceived security risk does have an effect on intentions to use smart home devices" [33]. The work of Zheng et al. [63] makes a strong case that users perceive privacy and security only as a secondary priority, and their opinion on these issues is strongly influenced by the benefits and conveniences a device can provide. This observation even extends to granting other entities access to personal data if this access might bring personal benefits [63]. The acceptance of potential risks could stem from the inability of most users to name concrete real-world consequences that can potentially result from a lack of security in smart homes [27, 35].

Continuing with the example of personal voice assistants from earlier, a 2019 study showed that almost half of Amazon and Google smart speaker users were unaware that their voice recordings are permanently stored on the device [42]. In general, users seem to be uneducated about what data is collected by their devices and think that sensitive data like health and financial information is not collected by a device, even though it is collected and even shared with third-party entities [8]. This lack of awareness is caused in large parts by the mismatch between the mental model of a smart home and the real world, as users with a more sophisticated mental model of their smart home also develop better threat models [62]. A similar mismatch can be observed between the users' perception of data practices and the actual privacy policy of IoT devices [8, 9].

Another big influence on the adoption process and user behavior with IoT devices is *Trust* [44]. Trust was identified as an important factor when it comes to the willingness of consumers to provide information to smart home systems [1]. Trust can stem from several sources such as brand familiarity [63], brand reputation

[63], and previously established relationships with brands [36]. Users often falsely assume that IoT devices already include all necessary privacy protections, so no further actions are needed [63]. However, this trust is not always well-founded, as even reputable companies can face data breaches and misuse of personal information *(see Section 2.1)*.

Ultimately, smart home users highly value security, but they often overlook potential privacy issues [17]. This is partly caused by the complexity of privacy information [50]. To reduce this complexity some sources suggest the use of standardized labels [23, 24] that make information more accessible and easy to understand. The immediate convenience [58, 63], lack of awareness about data collection practices [8, 42] and their real-world consequences [27, 35] contribute to the problem. Trust is influenced by brand familiarity and reputation and plays a crucial role in the adoption process of IoT devices [1]. However, trust also often leads to false assumptions that adequate privacy protections are already in place [63]. These findings show the gap between user perceptions and the real-world implications of privacy and security risks in smart homes.

2.3. Privacy in Shared Spaces

When considering privacy issues in smart homes, it is crucial to view these environments as 'shared spaces.' Often, multiple individuals live in one household, but usually, only one person configures the smart home devices, affecting the privacy of all occupants. This presents a unique challenge: how can a system inform secondary users and bystanders effectively about privacy? Generally, smart home users can be categorized into two distinct groups, introduced by Koshy et al. [34]:

Pilot User: "A user who takes on the responsibility of installing devices in the home and programming custom routines for them, and uses them regularly in their daily life" [59] [1].

Passenger User: "A user who's daily life is impacted by smart devices in their home (either through usage or through someone else's usage) but did not set up or program the devices in their home" [59] [1].

This categorization aligns with a similar grouping found in other sources: the *primary user*, who has full control over a smart home device and usually sets it up, and the *secondary user*, who interacts with the device but does not have full control [2, 36]. Typically, secondary users don't have a way to protect themselves against monitoring by the primary user [2].

Additionally, there are bystanders, like visitors or employees. Lau et al. [36] define these users as *incidental users*, that may not be aware of the device or don't fully understand its functionality.

This dynamic often originates from one partner in a relationship being particularly interested in smart home technology and considering it and the tasks revolving around it as a hobby [52]. The passenger/secondary user then often doesn't get much of a choice, as their partner may have already pursued that hobby before they met [52]. This situation, as described by Geeng and Roesner [26], results in one person having "access to vastly more functionality (including the ability to set permissions for functions co-occupants can use) and more information (such as knowing when someone opens and closes a smartlocked door)" [26], while the other doesn't receive the same benefits. In drastic cases, smart home technology was even misused as a tool in the context of intimate partner abuse [38], highlighting the need for clear and easy-to-use privacy controls for all stakeholders.

This division can result in "asymmetries of knowledge, control, and power dynamics between different user groups" [5], which can lead to privacy tensions between the different user types [36]. For example, Albayaydh and Flechais [5] found that household employees in Jordan often feel mistrusted by the use of smart home devices, with one participant even admitting to putting more effort into their work due to the presence of security cameras. In a similar study about the perspective of nannies on surveillance, Bernd et al. [13] found

[1] This definition was sourced from additional supplementary material provided by Windl et al. [59] upon request.

that most participants view a lack of disclosure about surveillance as a breach of trust, confirming the results of Albayaydh and Flechais [5]. Regardless of these strong feelings, most incidental and passenger users felt powerless to do anything because of existing power dynamics [5, 13]. This dynamic also shows in the context of Airbnb, where users expressed concerns about being spied on or discriminated against by the host [43].

In recent work about smart home privacy from the perspective of owners and bystanders, it was revealed that a major reason why smart home owners do not inform bystanders about their privacy practices is that they do not fully understand them themselves [7]. While 35% of interviewed smart homeowners agreed with the statement that "visitors have no privacy rights in my smart home", 45% of owners disagreed with it [7]. On top of this, 25% perceived the disclosure of privacy information as unnecessary, while 72% of bystanders reported feeling uncomfortable if their data is collected by other people's smart homes [7]. This further highlights the dilemma that users feel that they have the right to set up whatever devices they want in their own home [19], yet they don't have an easy way of informing others about the resulting privacy implications.

The importance of considering other stakeholders than the primary/pilot user is highlighted by the fact "that almost everyone at least sometimes experiences being an incidental user" [19]. Complementary, Thakkar et al. [55] suggested *Easy Access*, as a key design dimension for privacy awareness mechanisms: "privacy awareness mechanisms should be easily accessed by both users and bystanders" [55], which could help reduce the gap between pilot and passenger users.

In summary, privacy issues in shared environments like smart homes present complex challenges because some users do not have the same access to the controls of smart home devices as others [26, 52]. The difference in knowledge, control, and power among different groups [5] can lead to privacy tensions [36] and feelings of mistrust [5, 13], especially among secondary users and incidental users, with smart home devices sometimes being used in unethical ways [38]. These studies show the need for easily accessible privacy controls and information that is available to all user types, instead of only the pilot user of a system.

2.4. Approaches to Enhancing Privacy & Security Awareness and Control in Smart Homes

The next logical question one needs to ask themselves is, "how can we improve end-users' awareness and control of privacy and security in smart homes?". As explored in *Section 2.2*, privacy information is often presented in ways that are difficult for users to access or understand. Complementary to this, present approaches to privacy management "can lack immediacy of feedback and action, tend to be complex and non-engaging, and are inconsistent to users' natural interactions with the physical and social environment" [46], highlighting the need for further research in the area.

The work by Jin et al. [30] suggests that users primarily rely on physical-layer approaches for ensuring privacy, including the use of blocking mechanisms (e.g., for security cameras) or binary mechanisms like on-off switches. Building on this Do et al. [22] developed a *smart webcam cover* that requires users to actively uncover their webcams when they want to use them instead of having to cover them when they do not. Their results show that this automatic approach was viewed as way more effective compared to manual webcam covers [22].

This 'physical' approach can be extended to the concept of *Tangible Privacy*: "Tangible privacy mechanisms provide people with a way to clearly and unambiguously control and discern privacy states of IoT devices in their vicinity" [4]. The '*PriKey*' tangible interface developed by Delgado Rodriguez et al. [21] achieves this by grouping sensor types to represent different privacy choices: for each room, users can turn off the sensing capabilities (*video*, *audio*, and *presence sensing*) of all present devices, thus simplifying privacy management by reducing the amount of information and the number of devices that need individual attention [21]. In their recent work, Windl et al. [60] proposed a tangible smart home dashboard as a central hub for all smart home devices, raising privacy awareness by informing users about each device's type, location, connectivity, and

sensors. The results show that the "dashboard raised awareness of the devices' presence and capabilities for the device owners and visitors" [60]. Tangible privacy mechanisms have been shown to improve perceived trust in a system as well as usability [3] and are perceived by users as more engaging and fun [21].

Other approaches leverage the use of 'Hubs' as central junctions for communication in smart homes. By using a hub as a gateway that all device communication, both between devices and with third parties, has to pass through, decisions about privacy can effectively be centralized [53]. In an effort to increase transparency for data processing in smart homes Jin et al. [31] developed '*Peekaboo*,' a smart home hub that requires developers to declare the data collection behavior in the form of 'manifests' similar to the way permissions are handled on Android operating systems. Because all privacy manifests that can be downloaded to the hub need to be text-based and use a standardized set of operators, users are provided with a less cryptic way to inform themselves about data flows inside their smart home [31].

Privacy awareness can be raised by different methods like physical-layer approaches [22], tangible privacy mechanisms [21, 60], and hub-based solutions [31, 53]. Because physical-layer approaches, such as blocking mechanisms, provide straightforward access to privacy controls [22, 30], users often rely on them to ensure the safety of their data. Tangible privacy mechanisms offer intuitive and engaging ways for users to manage their privacy, leading to an improvement in perceived trust and usability [3, 21]. Hub-based solutions centralize privacy decisions, by implementing hubs as central junctions for communication in smart homes [53]. Despite recent advances, the field is still developing, especially the concept of 'Tangible Privacy' should be explored further, as it was only formally defined in 2020 [4].

2.5. Summary and Research Questions

While IoT and smart home technology get increasingly ubiquitous, users lack the ability to inform themselves [23, 45, 49, 50] and others [7, 19] effectively about privacy-related topics. This results in most users being unaware of data collection practices of their smart home devices [8, 42], false trust towards manufacturers [36, 63], the perception of privacy as a secondary issue [58, 63] as well as imbalances between pilot and passenger users [5, 13, 26, 38, 43, 52].

Based on these findings, we developed a novel smart home eco-system that gives users more granular control over their privacy and security in smart homes. Our work expands on the previously established concepts of '*ConnectivityControl*' [24, 56] and '*SaferHome*' [59], supporting the conclusion of Windl et al. [60] that future smart home systems should emphasize both control and awareness, rather than focusing on a single dimension. In the following sections, this concept will be described in detail and the results of an in-the-wild study with four households will be presented and analyzed. Overall, the following research questions (*RQs*) are addressed:

RQ1: What effect does the system have on the privacy awareness of users? Information and control about privacy are often only available to one user (the pilot user), while other stakeholders (passenger users and incidental users) do not receive the same benefits [26]. We present a tangible smart home dashboard that lets users (1) map out their smart home in the form of a floor plan to provide information about the type and location of smart home devices, (2) define individual privacy states for every smart home device in their network using a haptic input and (3) visualizes data flow in real-time to raise awareness about privacy.

RQ2: Do users prefer tangible or digital privacy controls? Users can either change the privacy state for each device on the tangible dashboard or use a web GUI to achieve the same effect.

3. System

We developed a novel smart home ecosystem that enables users to gain more control over privacy in their smart home while raising awareness for privacy at the same time. This chapter will briefly describe the ground-laying concept that includes both the tangible smart home dashboard as well as the '*PrivacyHub*' [48], the digital counterpart of the physical dashboard, before providing detailed information about the technical aspects of the smart home dashboard. The code, CAD files, and Gerber file for the prototype are included in the supplementary material of this thesis and can also be found on GitHub[1].

3.1. The Concept

To give the user more control over their privacy, we implemented a state-based system, based on the work of Feger et al. [24]. For each smart home device the user can decide individually how they want it to communicate: In *local*-mode the devices are only accessible within the same network, in *online*-mode the devices can be accessed from outside the home network using a password-protected website and in *online-shared*-mode the devices can also be accessed by paired third-party hubs like e.g. Alexa. All states are visualized in *Figure 3.2b*.

The dashboard *(see Section 3.2)* with its grid of 16 by 16 plugs, can be used to map out the floor plan of a household using string. On this floor plan the users can then place proxies *(see Section 3.3)* which represent smart home devices. These proxies can be used to change the privacy state of their respective device, while also providing information about the current state on a small display. The dashboard automatically detects the position of the proxies that are plugged in and communicates with the hub to display real-time data flow between the devices using integrated LEDs. The visualizations always flow from a proxy that represents a smart home device to the proxy that represents the hub or vice versa and are displayed in real time. We aim to raise privacy awareness of pilot users, passenger users, and incidental users, by providing information about the type and placement of smart home devices in a household, while also helping them understand when and how smart home devices communicate.

The hub acts as the main control unit of the system that lets users control their smart home devices and set privacy states. It also sends information about the data flow of the eco-system to the dashboard for visualization. The communication architecture between the tangible dashboard and the hub is visualized in *Figure 3.1*.

3.2. The Dashboard

The dashboard, at its core, consists of 16 custom-made printed circuit boards (PCBs) that were taken over from the '*SaferHome*' [59] prototype, with a grid of four-by-four DuPont plugs on each. The PCBs (from this point onward called tiles) are arranged in a four-by-four grid and daisy-chained together (*see Figure 3.2a*),

[1] `https://github.com/Phlipinator/SmartHome-Dashboard`

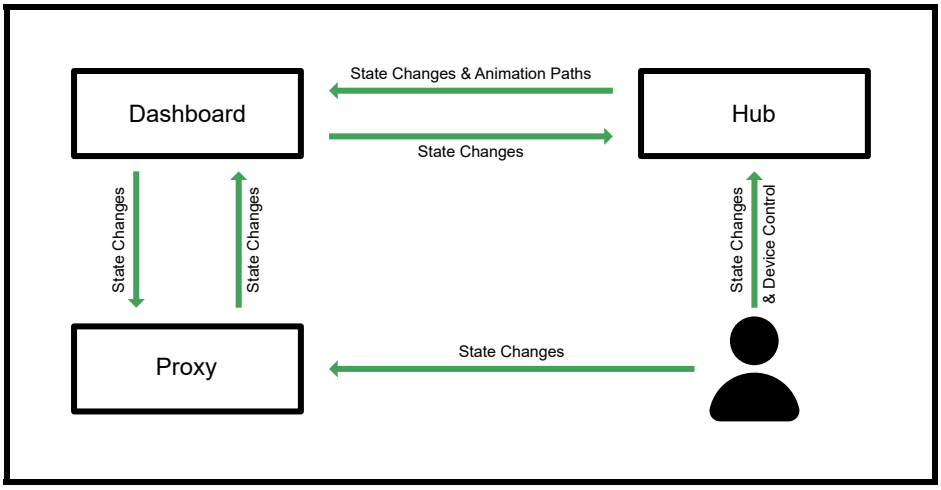
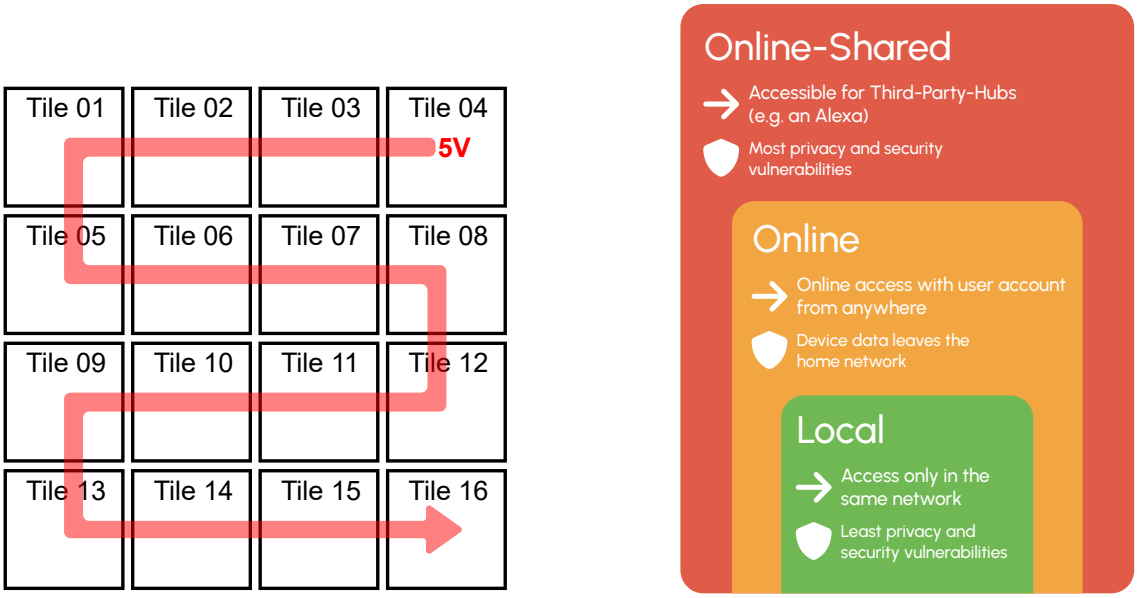


Figure 3.1.: The communication architecture in the smart home ecosystem



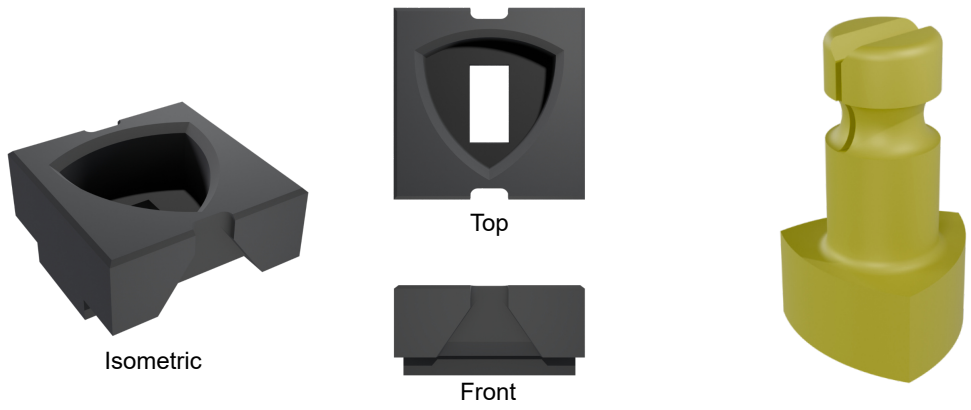
(a) **(b)**

Figure 3.2.: Figure a) shows the arrangement and electricity flow of the dashboard tiles, and b) shows the different privacy states

resulting in 256 plugs on the dashboard. From the back, the first tile is injected with *5 Volts (V)* at *3 Ampere (A)*, which gets transferred to the rest of the tiles. The functionality and the build process will be described in more detail in the following sections. The final prototype can be seen in *Figure 3.8*.

3.2.1. CAD

The dashboard was planned and constructed in *Fusion360*. A cross-section of the design can be seen in *Figure 3.4*. The tiles get sandwiched between a piece of wood in the back and two laser-cut plastic sheets in the front, with the addition of small silicon bumpers on both sides to help protect the resistors and ensure a



(a) **(b)**

Figure 3.3.: Figure a) shows the brick from different angles, and b) the pole that is used to secure string on the dashboard

safe placement. Spacers are positioned on all four sides of the dashboard that hold the tiles in place between the back plate and the plastic sheets. Each plug needs a designated LED to visualize the data streams on the dashboard. To avoid the inefficiency of soldering 256 individual LEDs, high-resolution LED strips (144 LEDs per meter) are placed on the laser-cut plastic sheets between the rows of plugs and wired together in a snake pattern, similar to the wiring of the tiles seen in *Figure 3.2a*. LED covers were constructed to conceal the areas where the LED strips thread through the plastic sheets and the back plate. These covers are also used to screw the front and back of the dashboard together. To make connecting proxies easier in the future, small bricks (*see Figure 3.3a*) with a key-lock system were designed to help align the proxies perfectly. The bricks were 3D printed individually to mitigate any inaccuracies from the soldering of the plugs and ensure a perfect fit of the guide system. Since the resolution of the LED strips did not perfectly align with the spacing between plugs, the bricks are designed with a light channel (*see Figure 3.3a front view*) that ensures at least one LED is always encapsulated. The light channel then guides the light to appear as a single, centralized source regardless of the LED placement.

Because up to this point, the plastic sheets are only screwed to the back plate at the sides through the holes in the spacers (*see Figure 3.4*), the plastic sheets are sewed to the back plate through unused mounting-holes in the PCB design of the tiles using fishing line. This prevents the plastic sheets from bending when proxies are removed from the dashboard. The bricks are then glued to the plastic sheets using double-sided tape and the dashboard gets encapsulated in a wood frame, to hide the electronic components and the wiring on the back. Finally, small poles (*see Figure 3.3b*) were designed and 3D printed that fit in the key-lock system of the dashboard and can be used to visualize floor plans with string.

3.2.2. The Tiles

Each plug features eight connectors in the order visualized in *Table 3.1*. **GND** and **5V** are used to power the plugged-in proxy, while **SCL** and **SDA** were initially used for I2C communication. **ROW** and **COL** have different voltages depending on the row and column they are on within a tile: the voltages on the ROW-pin are staggered from 5 V to 0 V with four steps from top to bottom and the voltages on the COL-pin are staggered the same way from left to right. These two pins are used to obtain relative position information by the proxy. Lastly **TILE** is used to obtain information about the tile, the proxy is plugged into. The voltage on the TILE-pin is staggered from 5 V to 0 V with 16 steps, representing the 16 tiles. With the relative position

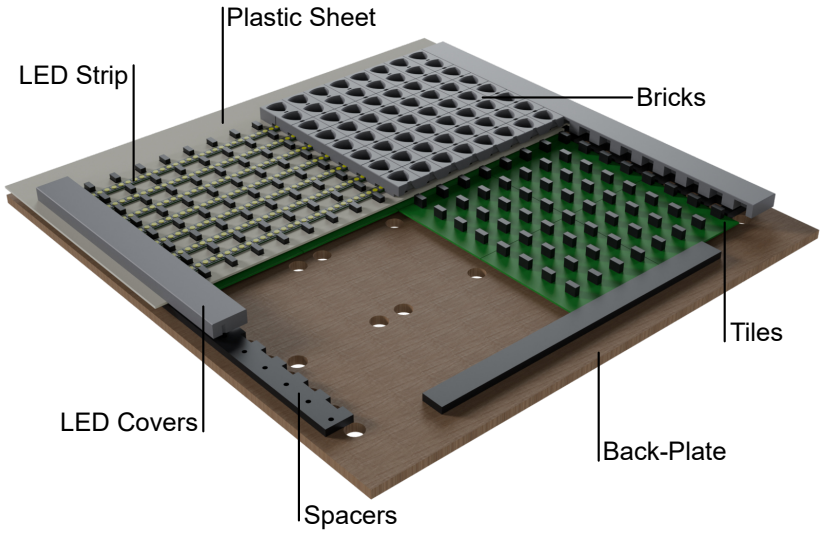


Figure 3.4.: A cross-section of the dashboard design

information from the ROW and COL-pin combined with the information from the TILE-pin, the system is now able to calculate the absolute position of a proxy on the dashboard. The different voltages on the COL and ROW-pin are achieved by reducing the input voltage (5 V) with resistors to get four distinguishable steps on each tile, for the TILE-pin the voltage is carried over on a separate line from tile to tile (*see Figure 3.2a*) and reduced with resistors between each one, resulting in 16 distinguishable voltage levels.

GND	5V
SCL	SDA
ROW	COL
	TILE

Table 3.1.: The layout of the eight-pin DuPont plugs on the dashboard

3.2.3. The Code

The code for the dashboard runs on a *Raspberry Pi 4B* and is organized in a class-based system. Initially, the communication between the dashboard and the proxies was planned to use the I2C-protocol, but because of several limitations regarding flexibility as well as the unreliability in such a large circuit, it was replaced with MQTT. The Raspberry Pi is connected to the internet via LAN and simultaneously hosts an access point for the proxies to connect to. This reduces the effort to set up the system in a new environment, as the proxies do not need to be initialized with new W-LAN credentials every time.

The *proxy*-class represents individual proxies on the dashboard, stores their values (position and state), and contains functions to calculate the absolute position of a proxy on the dashboard from the three voltage values as described in *Section 3.2.2*. The *config*-class is used to store information about what voltages correspond with which positions and how to calculate the absolute position from the relative position information, in the form of lists. The *logger*-class is used to write log messages to the console and into log files for error handling. The *messageHandler*-class contains most of the logic for the dashboard: first, it subscribes to all

relevant MQTT topics which are a general animation topic for the hub, an overriding topic for the hub to handle manual position overrides, and two update-topics per proxy, one for the proxy and one for the hub. Then all incoming messages get handled accordingly. This includes updating the state and position data for the proxy objects, handling manual position override data for the proxies, as well as the animation of data paths between proxies. Finally, the *lightController*-class is responsible for sending information about LED animations from the Raspberry Pi to an *ESP32 microcontroller* via USB-serial. The *lightController*-class also features a queue system that ensures the correct handling of multiple animation messages in a short time. All the above-mentioned classes are then initialized and executed in the *main*-file.

As previously described, the LEDs are controlled by an *ESP32 microcontroller*, which receives messages from the Raspberry Pi via USB serial. Initially, it was planned for the Raspberry Pi to directly control the LEDs, but due to issues with the precise timing required to control an LED strip with a total of 1151 LEDs on it, the use of a microcontroller with dedicated timing control was necessary. Because the constant powering of the LED strip caused a lot of heat and an electrostatic field that could potentially cause problems with the communication (noticeable when using I2C communication), a relay was introduced that only powers the LED strip when it is actually needed. The *ESP32* listens for messages and can handle three types of animations: (1) a plug-in animation that lets the LEDs adjacent to a coordinate pulse six times, (2) a path between two coordinates that gets repeated six times, and (3) a start-up animation that signals that the system has finished booting. At the core, the code features a two-dimensional array with 16 by 16 fields that represent the dashboard. Each field contains either one or two LED positions that can be used to animate data on the dashboard.

3.3. The Proxies

The proxies are used to represent smart home devices on the dashboard and give the user control over the privacy states. The system is based on the *ESP32* platform and features a custom PCB, a round display, and an incremental encoder which will all be described in more detail in the following sections. The final prototype can be seen in *Figure 3.8*.

3.3.1. CAD

Like the dashboard, the proxies were planned and constructed in *Fusion360*. A cross-section of the design can be seen in *Figure 3.5*. The design features a 3D-printed housing that can be screwed together to allow easy access to the microcontroller after the assembly. The display is connected to the PCB via a wired connection with a detachable socket and screwed to a 3D-printed mount, which is then screwed onto the PCB. The incremental encoder, which is used as the haptic input modality of the user, is also screwed and soldered to the PCB, and the microcontroller is soldered in place on the PCB. The plug consists of seven cables with crimped male-jumper-wire connections at the end, which are soldered to the PCB, then placed into an eight-pin DuPont plug and glued into the bottom part of the housing. Finally, the PCB gets mounted onto three designated stilts on the bottom part of the housing and secured in place using M2 screws and nuts. After the top and bottom parts of the housing are screwed together, the 3D-printed ring cover can be pressure-fitted over the incremental encoder. This ring provides a better surface to grip and also covers up the wiring and mounting of the display.

3.3.2. The Wiring

Because the design of the proxies requires a lot of connections, a custom PCB was built to account for the small form factor of the device. A wiring diagram of the system can be seen in *Figure 3.6*. Originally the '*SaferHome*' prototype [59], was developed to use the *Arduino Nano* as a platform for the proxies, however

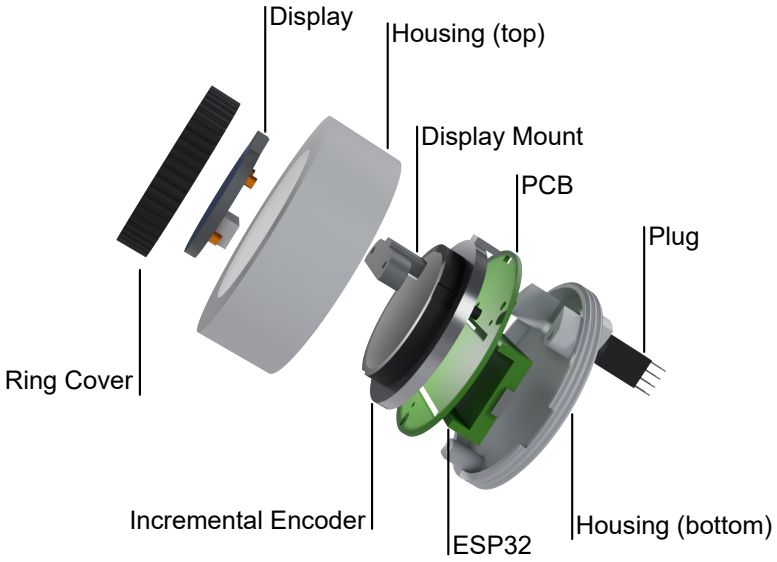


Figure 3.5.: A cross-section of the proxy design

with the increased capabilities of the system, the *Arduino Nano* no longer had enough flash-memory and processing power and was therefore replaced with an *ESP32*. The Arduino Nano's internal logic operates at 5 V, while the ESP32 only operates at 3 V. This causes a problem, as the position information gets represented in a range of 5 V to 0 V *see Section 3.2.2*. To solve this voltage dividers were introduced, to reduce the incoming voltage to a level that is safe for the ESP32 to read. For the ROW and COL-pin, a setup with $R_1 = 5.1\,\text{k}\Omega$ and $R_2 = 10\,\text{k}\Omega$ was used. Because the TILE-pin requires a higher resolution with 16 distinguishable steps instead of four, a setup with $R_1 = 6.8\,\text{k}\Omega$ and $R_2 = 10\,\text{k}\Omega$ was used. The resulting voltage can then be calculated with this formula:

$$V_{\text{out}} = V_{\text{in}} \frac{R_2}{R_1 + R_2}$$

3.3.3. The Code

The code for the proxies is written in *C++* and consists of two files: the *config*-file is used to store all parameter declarations and credentials, while the *ui*-file contains the main logic. The user interface (UI) (*see Figure 3.7*) was designed in *Affinity Designer* and then integrated into the code using *Squareline Studio*. As mentioned in *Section 3.2.3*, initially it was intended to use I2C for the communication between the proxies and the dashboard, which was then replaced with MQTT. As MQTT requires a W-LAN connection, the UI files had to be optimized to fit the 2MB flash memory of the ESP32. The W-LAN module of the ESP32 requires a lot of power during the boot-process, which caused voltage drops, that made it impossible for the proxies to boot when plugged into the lower half of the dashboard. To fix this, a power injection was introduced on tile twelve. When booting, the proxy first reads the three voltages for the position calculation, because the Analogue-to-Digital (ADC) capabilities of some of the used pins are not usable when the W-LAN module is used. After this, the proxy connects to the access point of the dashboard and establishes a connection to the MQTT-broker. It then publishes the three voltage readings and continues to listen for changes in the position of the incremental encoder as well as state updates from the hub. If a change is detected (either on

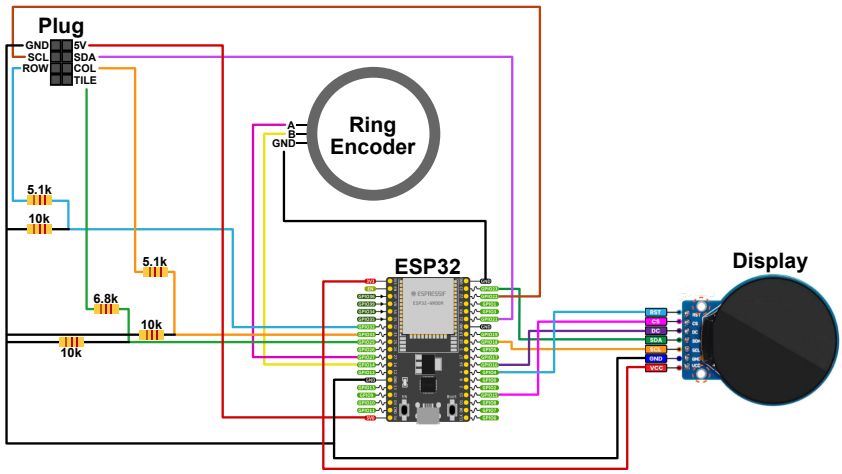


Figure 3.6.: The wiring diagram for the proxies

the MQTT-topic from the hub or in the position of the incremental encoder), the UI gets adapted accordingly, by turning the text elements to display the correct state. In the case of a change in the incremental encoder position, a state update also gets published via MQTT.

Figure 3.7.: The proxy user interface for a smart light

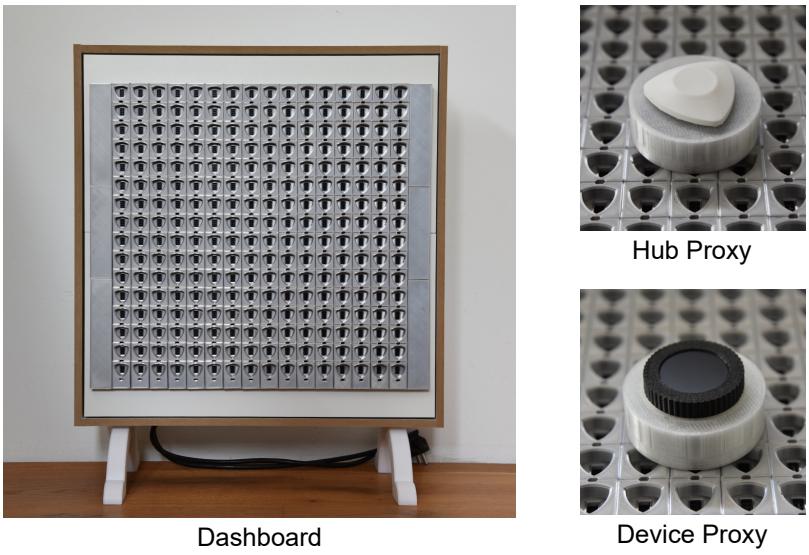


Figure 3.8.: The dashboard prototype and two proxy prototypes

4. Study Design

We carried out an in-the-wild study with nine participants in four households over the course of a month. Each household had two to three inhabitants and interacted with the system for seven to eight days. We chose an in-the-wild study design to ensure a realistic and natural interaction with the system and give users the chance to interact with it the same way they would with other smart home appliances. Our main goal was the evaluation of the system in terms of general usability, its effect on privacy awareness, and the comparison between tangible and digital controls.

4.1. Procedure

After a brief introduction, the participants were asked to sign a consent form, while the experimenters set up the system. This involved connecting the LAN and power for the dashboard and hub, as well as pairing three smart home devices and an Alexa smart speaker with the hub. We chose a smart socket, a smart door sensor, and a smart light because they are common in smart homes and to ensure that they would work with the hub, which we could not guarantee for devices the participants may already own. The participants were able to freely choose the location of all components, with the requirement that the dashboard should be placed at a location where it is clearly visible, which was mostly in the living room near the TV. After the initial setup was complete, the concept and core functionality of the system were briefly explained to the participants. This included the three privacy states and the use of the tangible dashboard. The participants were then asked to fill out a questionnaire about demographic data and other questions regarding their experience and user behavior with smart home devices (*see Appendix A*). Next, participants were asked to take part in a show-and-tell session, where the experimenters explained in detail how the system works. This included the use of the different user interfaces (local and online websites), the hub's functionality, and interacting with the dashboard by plugging in proxies, changing their privacy settings, and creating a floor plan. The participants were also instructed on how to do minor error handling in case the system stopped working, which mostly consisted of restarting different components. The participants were instructed to use the system as they saw fit but should interact with it at least once per day.

After seven to eight days, participants were asked to complete another questionnaire about their experience with the system, followed by an interview to discuss their feedback in more detail. The used material for the user study is attached in *Appendix A* and will be described in more detail in the following section.

4.2. Measurements

Because all participants were native German speakers, the questionnaires and the interview were conducted in German language. All referenced material can be found in *Appendix A* and is marked with red numbers for easier navigation.

In the demographic questionnaire, some general data about the user is recorded such as age, gender, profession, highest level of education, and the number of smart home devices in the household is collected. In question 1.0 the user needs to decide if they identify as a pilot or passenger user, based on the definition by Windl et al. [59].

All questions feature a six-point Likert scale ranging from '*completely disagree*' to '*completely agree*'. Questions 1.1 - 1.8 focus on the participants' general opinion on smart homes and their privacy awareness. The same questions were revisited as 2.1 - 2.8 after a week of using the system to assess any changes. Questions 1.9 - 1.17 comprise the *ATI* questionnaire developed by Franke et al. [25] to assess users' general affinity with technology. Finally, question 1.18 aims to get a rough estimate of how often the participants interact with smart home devices. This question also features a six-point Likert scale but uses the items '*multiple times per day*', '*once per day*', '*multiple times per week*', '*once per week*', '*multiple times per month*' and '*never*'.

After a week, the participants were asked to fill out the second part of the questionnaire, consisting of the questions mentioned above (2.1 - 2.8) and the *SUS* questionnaire [16] for both the hub (3.1 - 3.10) and the dashboard (4.1 - 4.10).

The interview (5.1 - 5.23) was conducted after the participants finished the second part of the questionnaire and consisted of a general part (5.1 - 5.11 & 5.23), a part for the hub (5.12 - 5.17) and a part for the dashboard (5.18 - 5.22). All questions were open-ended and aimed to generate qualitative data about how the participants used the system and the system's influence on privacy awareness.

During the test phase, all interactions with the system were recorded for a quantitative analysis. This includes device control and the change of privacy states both on the dashboard and in the hubs' UI.

4.3. Participants

Nine participants (five male and four female) in four households were recruited via convenience sampling. The age ranged between 25 and 54 (M = 31, SD = 12.89), and all participants received a compensation of 25€. The *ATI* scale [25] (ranging from one to six) resulted in a median score of 4.36, with a standard deviation of 1.15. On average, households had 11.25 smart home devices (SD = 8.46). Details about the households and participants are listed in *Table 4.1*. The configured dashboard for each household can be seen in *Figure 4.1*. In household one, only two smart home devices (the door sensor and the smart plug) were implemented, due to technical difficulties with the smart lamp.

Household	Number of Smart Home Devices	Participant ID	User Type	Age	Gender	Profession	Highest Level of Education	Technical Affinity
Household 1	20	P1	Pilot	53	M	Banker	Apprenticeship	5.22
		P2	Passenger	54	F	Housewife	Apprenticeship	2.33
Household 2	1	P3	Passenger	25	F	Scientific Assistant	Bachelor of Arts	3.78
		P4	Pilot	26	M	Working Student Social Media & Marketing	Vocational Diploma	4.33
Household 3	8	P5	Pilot	26	M	Editorial Journalist	Bachelor of Arts	4.78
		P6	Passenger	20	F	Working Student in Sales	High School Diploma	2.89
Household 4	16	P7	Passenger	26	M	IT Consultant	Master of Science	5.0
		P8	Pilot	25	M	Consultant	Master of Science	5.78
		P9	Passenger	24	F	Student (IT & Design)	High School Diploma & Apprenticeship	5.11

Table 4.1.: Household information and participant details

Seven participants (P1, P2, P4, P5, P7, P8, P9) reported using smart home devices multiple times per day, one participant (P3) used them once per day, and one participant (P6) used them multiple times per week.

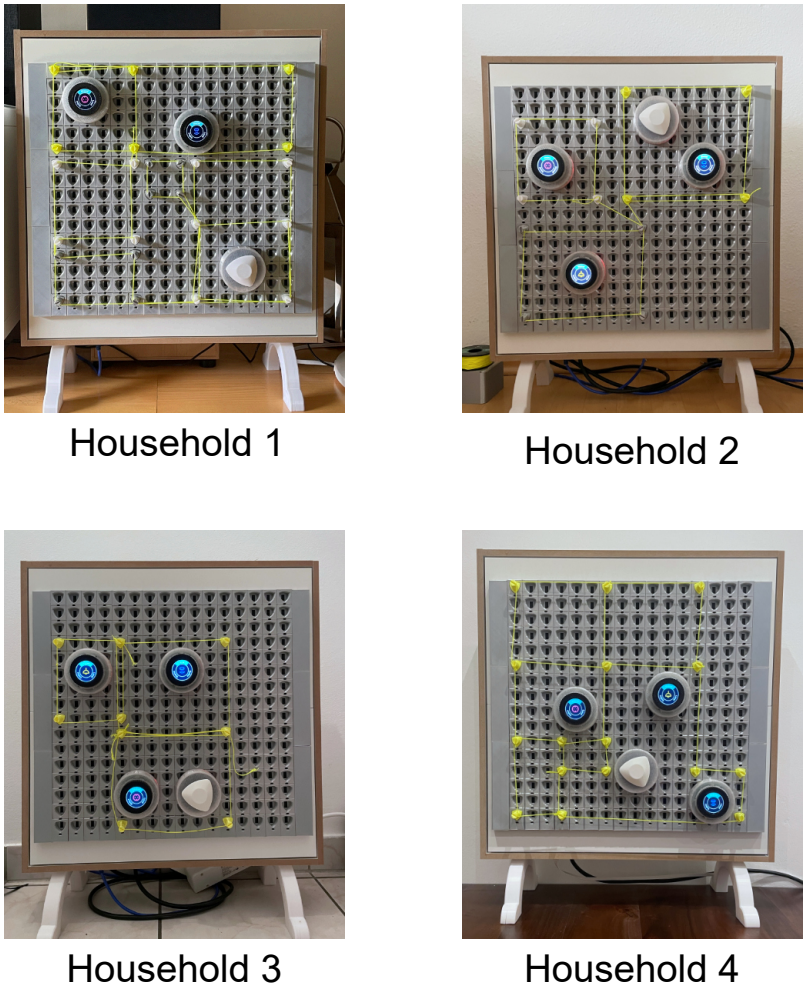


Figure 4.1.: The dashboard configuration of each household

5. Results

We analyzed the quantitative data collected from the system's database and questionnaires using Python and Excel and applied affinity diagramming [28] to the qualitative data from the interviews. To transcribe audio recordings from the interviews, we applied the whisper model[1], followed by manual corrections to address any errors. We used *Atlas.ti* to collaboratively code the interviews. First, two researchers independently coded the same interview and discussed the results to create a shared codebook. Using this code book we then coded the remaining interviews.

5.1. Quantitative Data

Due to the small sample size, the quantitative data should be considered a supplement to the qualitative results.

5.1.1. System Usability Score (SUS)

Because of a self-reported lack of interaction with the system, we excluded P2 from the SUS [16] calculations. The tangible dashboard received a mean SUS score of 81.56 (SD = 8.55), indicating a 'GOOD' (grade B) usability according to the scale developed by Bangor et al. [12]. The SUS score for each participant can be seen in *Figure 5.1*.

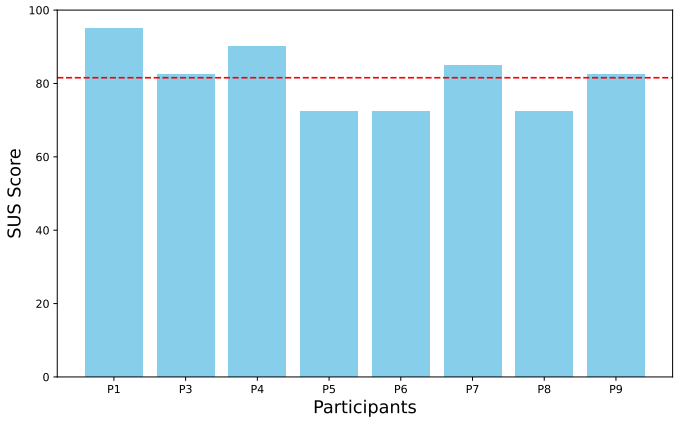


Figure 5.1.: The SUS score for all participants

[1] https://github.com/openai/whisper

5.1.2. Privacy State Change Location

The participants have utilized both the tangible and digital interface almost equally for state changes, with a minor tendency towards the digital interface. The relative distribution of the state change locations over all four households was 50.7% for the web GUI and 49.3% for the tangible dashboard. However, an overhang in digital or tangible use can be seen for individual households depending on preference *see Figure 5.2*.

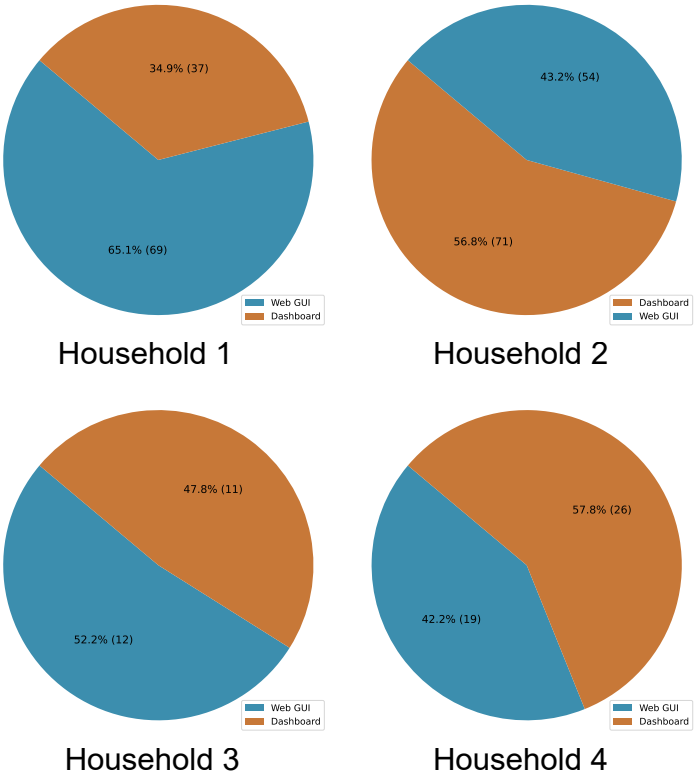


Figure 5.2.: The state change location of all four households

5.1.3. Smart Home Privacy

As described in *Section 4.2*, all participants answered eight questions regarding privacy in smart homes before and after the study. A translated version of these questions can be found in *Table 5.1*. Each question was answered on a six-point Likert scale ranging from '*completely disagree*' to '*completely agree*'.

Figure 5.3 shows the distribution of the answers from all participants before and after the study. We performed a t-test which returned a p-value lower than 0.05 for questions Q3, Q7, and Q8, indicating a statistically significant difference. The mean value of Q3 decreased from 5.33 to 4.56, indicating that after the study users care less about the features that a smart home system can provide than before. This decrease could also mean that users no longer prioritize the features of smart home systems over its privacy, but because the value of Q4 decreased as well and shows no statistically significant difference, this interpretation is less robust. The mean value for Q7 increased from 2.67 to 3.78, which suggests that users feel more capable of protecting their private data in smart homes through the use of the system. The mean value from Q8 increased as well from 2.56 to 3.33, indicating that the system educated users about the way data flows in a smart home. For Q1 the t-test returned a p-value of 0.051, which is only slightly above the conventional

ID	Questions
Q1	I am very familiar with smart home systems.
Q2	Data privacy is very important to me.
Q3	The range of features is the most important aspect of smart home devices to me.
Q4	Data privacy is the most important aspect of smart home devices to me.
Q5	I feel that I have control over my private data in my smart home.
Q6	I am very concerned about my private data in my smart home.
Q7	I know how to protect my private data in my smart home.
Q8	I feel that I am well informed about what happens to my private data in my smart home.

Table 5.1.: Questions related to smart home systems and data privacy.

threshold of 0.05. This shows a trend that the system raises the perceived familiarity of users with smart home systems, although the result falls just short of statistical significance. Interestingly, the mean value for Q2 shows almost no difference before and after the study, which could mean that the importance of privacy is a fundamental opinion that doesn't get easily changed through the use of a system.

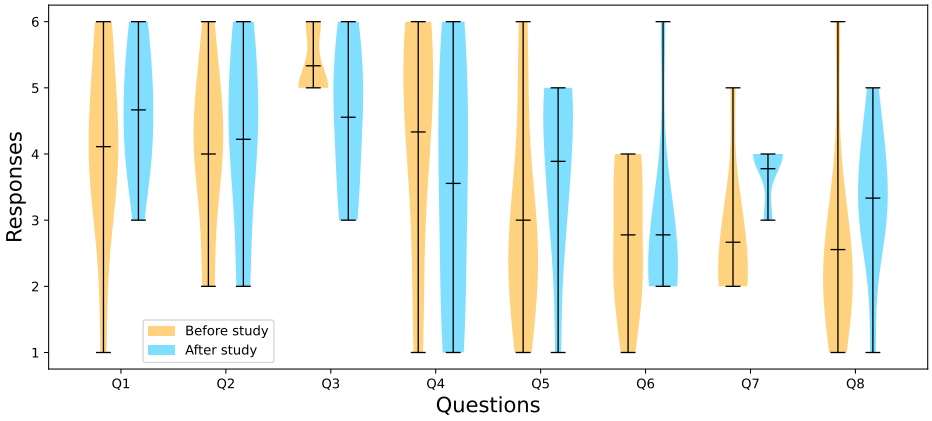


Figure 5.3.: The answers to the eight smart home privacy questions before and after the study of all participants

Figure 5.4 shows the distribution of the answers from only passenger users before and after the study. A t-test returned a value below 0.05 for questions Q1, Q3, Q7, and Q8, indicating a statistically significant difference. The mean value of Q1 increased from 3.2 to 4.2, suggesting that passenger users feel more familiar with smart home systems in general after taking part in the study. The mean value of Q3 decreased from 5.2 to 4 showing that, similar to the results of all user types, passenger users care less about the features a smart home system can provide them with after the study than before. Because Q4 again showed no statistically significant difference, the interpretation that the system had an effect on the balance between the prioritization of features and privacy is not very robust. Similar to the results of all user types, the mean value of Q7 increased from 2.2 to 3.8, and the mean value of Q8 from 2.2 to 3.2. This indicates that passenger users feel more in control over their private data in smart homes and feel more educated about the data flow after the study compared to before the study. For Q6 we found an increase from four to six for P2, which is curious considering she reported not interacting with the system. This could mean that the visualization of the dashboard was enough to cause a change in how P2 views the importance of data protection.

A t-test for the results of the pilot users showed no statistically significant difference for any of the eight questions, however, the trends were similar to passenger users. Considering pilot users have access to vastly more control and information about smart home environments than passenger users, this result is not surprising.

With the interpretation of these results, it is important to keep in mind that all these values are subjective assessments by the participants and do not necessarily accurately represent the real-world.

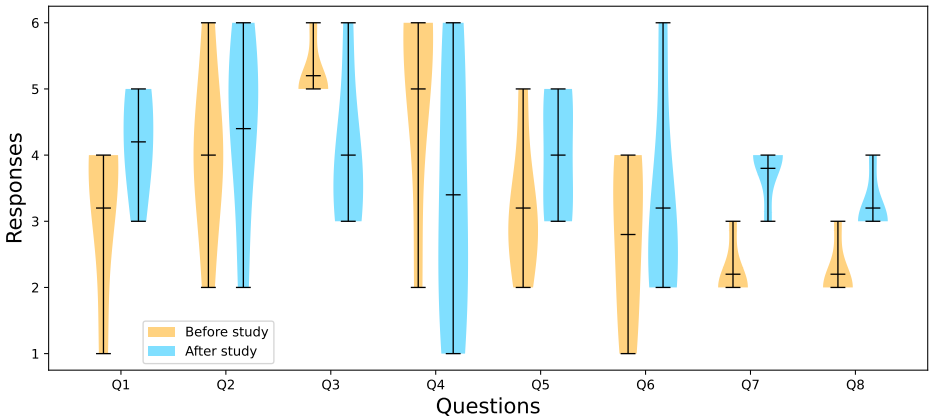


Figure 5.4.: The answers to the eight smart home privacy questions before and after the study of the passenger users

5.2. Qualitative Data

The coding resulted in a total of 151 individual codes, which were clustered into 23 groups and five themes using a bottom-up approach. The themes *Privacy Awareness*, *Presentation*, *Interaction*, *Integration with Commercial Systems*, and *Requested Features* will be detailed in the following sections. The analysis is focused on the aspects related to the tangible dashboard and the overall system, excluding parts specific to the PrivacyHub. Since all interviews were conducted in German, direct quotes will be translated. In the following sections the term '*system*' is used to refer to the system as a whole (PrivacyHub *and* tangible dashboard) and the term '*dashboard*' or '*tangible dashboard*' is used to refer to the prototype developed for this thesis.

P2 reported that she was too scared to use the system and that she generally leaves all technical tasks to her husband (the pilot user of the household), which is why P2 will not appear frequently in the results.

5.2.1. Privacy Awareness

Evaluating the impact of the system on users' privacy awareness is a key objective of this thesis. This section explores user perceptions and experiences related to privacy awareness after interacting with the system.

Seven users (P1, P3, P4, P5, P6, P8, P9) implied that the system as a whole raised their privacy awareness, while only P7 stated that the system did not affect his privacy awareness with no indirect implications that it did. For example, P1 stated "*basically, it just gets you to think about [privacy]. You connect some device, it runs relatively easily, and you already have the next thing connected to the network. And you can never be a hundred percent sure, what it is actually doing.*" Interestingly, when asked directly if the system raised their

privacy awareness some users (P8, P9), denied that it did, but proceeded to explain how the system made them think more about privacy issues in smart homes, which is a rise in awareness. Only two users (P1, P3) explicitly stated that the tangible dashboard affected their privacy awareness, with P3 stating "*I think it's cool that this dashboard somehow brings [privacy] to awareness and makes it really manageable for things that I otherwise don't understand*", while also reporting that the dashboard made privacy more graspable for her. When asked about the impact of the dashboard's data visualization on their privacy awareness, five users (P3, P4, P6, P8, P9) stated that the visualization had a direct impact, while three users (P1, P5, P7) said there was no direct impact. P7 stated that he did not make a conscious connection between the LED animations and the data flow in a smart home and P8 said that he acknowledged the visualizations but they did not cause any change in his behavior. P5 clearly stated that he is aware of the privacy issues that certain devices of his smart home have, but prioritizes the convenience they can offer: "*I am very aware of the situation with the data and have consciously chosen the largest feature set and the least security*". In addition, P5 explained that he would change his behavior regarding privacy if it was easier to do with current systems. P7 and P8 also stated that privacy is not really a concern to them.

Overall, the system positively influenced privacy awareness for most users, as supported by responses indicating increased consideration of privacy issues. These findings align with the quantitative results regarding privacy awareness in smart homes presented in *Section 5.1.3*.

5.2.2. Interaction

The participants were able to interact with the system either through the tangible dashboard or the digital interface of the PrivacyHub. This section presents users' preferences for different interaction types and the perceived usability of the tangible dashboard and the system.

Five participants (P3, P4, P5, P7, P8) explicitly mentioned that they used the dashboard to change privacy states, while four users (P1, P3, P4, P9) reported using the web graphical user interface (GUI) for these adjustments. These findings align with the data presented in *Section 5.1.2*, which shows an equal distribution between the state change locations. Two of the participants from household four (P7, P8) reported, that they did not use the web GUI to change privacy states. Three users (P1, P3, P5) mentioned that they used the state changes to check if the system is still working and P8 also used it to try to fix connection issues with his third-party hub, while the members of household two (P3, P4) noted that they changed the privacy states for fun. While this isn't inherently a bad thing, it still shows that users did not see the need to change the privacy states of their devices to control their privacy. P1 and P6 even perceived the state changes as unnecessary as a whole because they did not feel a need to adjust any privacy settings on their devices. The members of household three (P5, P6) were heavy users of the 'Alexa' smart speaker and therefore explained that they mostly used the online-shared state so they are able to control the smart-plug and the smart-light via voice. P3 also expressed primarily using online and online-shared because it provides the biggest feature set, while at the same time explaining that the local state felt the most safe to her. P7 and P9 used the state system to restrict other household members' access to a device in a private room, highlighting the need for a system that supports multiple users. Two users (P8, P9) explained that they would define privacy states once for each device and then leave it at that, as they don't see a need for constant adjustments.

Five participants (P1, P2, P3, P4, P6) explained that they mostly preferred a digital experience over a tangible experience for convenience reasons, with P1 stating that he sees no advantage in a tangible solution. On the other hand, three users (P5, P7, P8) preferred the tangible experience, and five users (P3, P4, P5, P8, P9) stated that they liked a mix of both. Notably, P3 and P4, while favoring digital experiences for convenience, also appreciated the benefits of combining both digital and tangible elements. Complementary P7 expressed that once the user is familiar with the system a purely digital approach would likely be easier. When asked about the haptic component of the system, five participants (P3, P4, P7, P8, P9) expressed their appreciation with P7 stating "*That really awakened the playful child in me. Turning it was cool, it was fun (...).*" Two users (P1, P4) suggested that a tangible solution could be more suitable for people with less technical affinity, as it is easier to understand. However, we did not find a correlation between a low ATI score and a preference

for tangible interaction. Users with the lowest ATI scores (P2, P6) both preferred a digital solution for convenience reasons, although P6 mentioned that a tangible interaction feels more robust to her. P7 and P8 both stated that they think the tangible dashboard could also be a display. P8 later withdrew that statement: "*I find something like that naturally encourages more use, and in my eyes, it's also more attractive (...), and has more function, than if you just hang a display on the wall.*"

Two participants (P4, P7) mentioned that they found the system to have good usability, while three users (P5, P6, P7) stated the same about the dashboard's usability. This confirms the results from the SUS questionnaire presented in *Section 5.1.1*, which shows that users thought the dashboard has a generally 'good' usability. P6 mentioned that she had problems understanding the dashboard and P8 explained that he did not know how to fix errors with the system and that he found the name change of the 'online-shared' state to 'shared' on the proxy displays confusing. P4 implied that the system gives him a sense of control, especially with the use of smart speakers: "*Just like with Alexa, I have the option to opt in or out at any time.*"

Six participants (P3, P4, P5, P6, P7, P9) explained that they would use the system further after completing the study. P1 explained that he would use the system further if it was smaller (referring to the dashboard) and P8 stated that he would use the system if it could be integrated into 'Home-Kit'. Five users (P1, P3, P4, P5, P9) stated that they would recommend the system further with only two users (P7, P8) stating that they would not recommend it. All users agreed that the system is better suited for more technically experienced users, but P6 later stated that she could also imagine it for non-technical users like elderly people. P2 explained that she thinks using the system is a task for the pilot user and P7 stated that he thinks the system requires a very distinct user group: "*I would recommend it to people who are a bit more tech-savvy but still somewhat mindful of their privacy. You have to find a very specific target group, I think, who are not already very good at protecting their privacy.*"

Two users (P1, P4) explained that they think the dashboard could be useful for managing larger systems with P1 specifying that he thinks the dashboard could be used for easier maintenance for example in a commercial setting. Lastly, eight participants (P1, P3, P4, P5, P6, P7, P8, P9) stated that they thought the system felt safe, and P9 also described it as transparent.

Overall, the participants had different preferences for the interaction with the system. Some users prefer the convenience of a digital interface, others like the 'playful' aspect of the tangible interface and some stated that they prefer a mixture of both modalities. Users found the dashboard and the system had a good usability, confirming the results of the SUS questionnaire but some expressed the need for better onboarding with the dashboard as they didn't think it was self-explanatory. Most participants said they would continue using the system and recommend it to friends or family, indicating a demand for privacy control mechanisms in smart home systems.

5.2.3. Presentation

This section explores participants' perceptions of the dashboard's presentation.

Six participants (P1, P3, P4, P5, P7, P8) perceived the dashboard as useful, with two users (P1, P4) especially liking the design and three users (P1, P4, P7) especially liking the floor plan feature. While P4 thought the key-lock mechanism of the dashboard was easy to use, three users (P3, P5, P9) thought the pins felt fragile and could easily break. Three participants (P1, P3, P6) stated that they think the dashboard needs to be positioned at a central location of the household, where it is clearly visible.

Eight users (P1, P2, P3, P4, P5, P6, P7, P9) liked the data visualizations, with P7 stating that he thinks they could get annoying over time and P3 suggesting lowering the number of repetitions in each visualization.

Five users (P1, P3, P4, P5, P8) perceived the dashboard as a good visualization tool. P3 remarked that the dashboard made privacy more graspable for her: "*I think through the dashboard, I really recognized the value of the whole thing. It made it much, much more graspable for me what actually happens.*" P3 later also expressed a sense of empowerment through the use of the dashboard. P8 stated that he thinks the dashboard motivates users to engage with the system.

P1 and P3 both stated that the concept of the system made sense to them, but is not self-explanatory. Participants P1 and P4 liked the state system, with P1 specifying that he found the traffic light system easy to understand.

Participants generally found the dashboard to be useful and liked its design and features. The results show areas for improvement such as concerns about the durability of the proxy pins and ideas on how the data visualizations could be changed.

5.2.4. Integration with Commercial Systems

Several participants provided insights into their perception of trust in brands and privacy sensitivity based on device types and smart home solutions.

Five participants (P1, P4, P7, P8, P9) indicated that their trust in a system depends on the brand's image, with two users (P1, P8) specifically naming 'Apple' as a trustworthy brand. On the other hand, two users (P1, P4) stated that they consider 'Amazon' as a not trustworthy brand. Three users (P5, P6, P7) expressed that for them, the data sensibility depends on the device type, with P5 stating "*I don't really care if they know whether my light is on or not, even though something can of course be interpreted from it. A door sensor is different; it's data that definitely can't be misinterpreted (...). And that's why I rate it somewhat higher.*" P7 also stated that he does not consider the three used smart home devices as privacy sensitive. P1 noted that commercial smart home solutions give the user no control over their privacy: "*(...) you don't have the slightest control over what data flows and what kind of access is possible in your network.*"

5.2.5. Requested Features

In this section, we will present a list of features that the users requested for the dashboard or the system as a whole. The participants who requested the features are listed behind their request.

Requested features for the system

- A voice controller component to replace unsafe options like 'Alexa' (P5)
- An always-on option for devices that only work when they can communicate outside of the home network (P1)
- A main switch, that lets the user define privacy states for multiple devices at once (P1)

Requested features for the dashboard

- The dashboard should be smaller/thinner (P1, P2, P3, P6)
- A 'sleep mode' that dims the proxy displays when the system is not used for a longer time (P3, P4, P7, P8)
- Show the device status (on/off) on the proxy displays (P4)
- Add the color code from the privacy states to the proxy displays (P1)
- Add device controls (on/off) to the proxy displays (P8)
- Add a digital counterpart of the tangible dashboard to the web GUI (P8)
- Make proxies smaller, so more of them can fit on the dashboard (P8)
- Provide information about the dashboards' power consumption (P8)
- Add a more figurative explanation to the dashboard (P6)
- Visualize data leaving the network (P6)

6. Discussion

In this discussion, we interpret the findings of our study. We investigated the impact of a tangible smart home dashboard on user privacy awareness (RQ1) and user preferences for tangible versus digital privacy controls (RQ2). By analyzing the results, we aim to provide insights into how such a system can influence privacy practices and preferences within a smart home environment and give recommendations for the design of future systems.

6.1. RQ1: What Effect Does the System Have on the Privacy Awareness of Users?

Our study aimed to evaluate the impact of the system on users' privacy awareness, which is important given the increasing number of connected devices around the world. Our findings reveal that the majority of participants recognized a rise in awareness of privacy issues following their interactions with the system. Both the qualitative data from our interviews (*see Section 5.2*) and the quantitative data from the questionnaires (*see Section 5.1*) support this conclusion.

While seven users reported that the system raised their privacy awareness, only two users explicitly stated the same about the tangible dashboard. Still, five users thought the dashboard was a good visualization tool and eight users stated that they liked the data visualizations. As we presented participants with the system as a whole and did not introduce the tangible dashboard and the PrivacyHub as separate parts, we can partially credit the rise in privacy awareness caused by the system to the tangible dashboard. During the conceptualization of this thesis we thought of ways to mitigate the unequal control that different user types have over privacy in smart homes [5, 13, 26, 43, 52]. The pilot user [34] of a system usually installs smart home devices and has access to more controls and information than other users, creating the previously mentioned imbalance. For passenger users, we found a significant increase in the perceived familiarity with smart home systems in general and in perceived knowledge about how to protect and what happens with data in smart homes (*see Section 5.1.3*). One passenger user also explicitly stated that the dashboard gave them access to information they would otherwise not understand. While we found similar trends for pilot users, a t-test revealed no statistical significance. Given that pilot users already had access to more information and control in their smart homes than passenger users, this result is not surprising. Across all user types, our quantitative data also shows a significant increase in perceived knowledge about how to protect and what happens with data in smart homes.

The results of our study show that most users generally do not prioritize privacy, with some participants explicitly stating that privacy is not a concern for them. This observation aligns with the research of Wang et al. [58] and Zheng et al. [63], who also found that privacy is often not a primary concern for users [63] and that the perceived benefits of smart home devices are rated higher than their privacy risks [58]. Some participants expressed a desire for greater control over data privacy in their smart homes but were hindered by commercial systems lacking the necessary tools or the fact that a change in behavior would require a lot of work. This aligns with the work of Mehta [46], which describes current solutions to privacy management as often "complex and non-engaging" [46]. Previous work shows that trust in a system depends on brand familiarity [62], brand reputation [62] and the relationships that users establish with a certain brand [36]. Our results confirm this, as five participants reported that brand image is a factor that influences their trust in a smart home system.

Our results show that our eco-system, including the tangible dashboard, is effective in raising participants' privacy awareness. This suggests that well-designed interfaces, distinct privacy controls, and visualization tools can be effective in educating users about privacy. Systems should be designed to provide equal access to privacy controls and information for all user types instead of focusing on the pilot user. Because most participants still did not consider privacy a high priority, there is a need for further research about privacy awareness in smart home systems. Given this low priority, there may also be a need for stronger regulatory measures to protect user data in smart homes and increase the transparency of smart home systems.

6.2. RQ2: Do Users Prefer Tangible or Digital Privacy Controls?

During our study, we gave participants control over the data flow in their smart homes with the implementation of privacy states. This state system is based on the work of Feger et al. [24] and allows users to define individual privacy settings for each integrated smart home device. The participants could either interact with a mobile web GUI to change privacy states or use the tangible interface of the dashboard. Our findings show that the distribution between tangible and digital interactions was very balanced (*see Section 5.1.2*), with some users preferring a digital experience, others a tangible experience, and some a mixture of both options (*see Section 5.2.2*). This balanced distribution is noteworthy, considering that the digital interface is easily accessible from anywhere, whereas interacting with the tangible interface requires the user to be near the dashboard.

Our qualitative data (*see Section 5.2.2*) supports the equal distribution revealed by the quantitative data, with five participants stating that they used the tangible interface for state changes and four users stating that they used the digital interface. The work of Jin et al. [30] implies that users mainly rely on physical-layer methods to ensure their privacy. Some sources implemented this by making use of blocking mechanisms like a smart webcam cover [22] or the ability to disable or enable different sensing capabilities like video, audio, or presence sensing [21].

In their work about tangible privacy Delgado Rodriguez et al. [21] found that the tangible prototype was "perceived as more fun, engaging, encouraging and benevolent compared to the app" [21], which aligns with the results of our study. On the other hand, the digital solution was preferred for convenience reasons by roughly half of the users, which is also similar to the results found for the 'PriKey' tangible interface [21]. Five users liked a mixture of both a tangible and a digital approach, as was presented in our study. Our results are supported by a recent survey (N = 444) that found "participants rated their preference for tangible interactions with privacy mechanisms overall neutrally" [20], however they also agreed that tangible privacy controls raise awareness on privacy intrusions [20].

The SUS questionnaire returned a mean value of 81.56 (*see Section 5.1.1*), showing that users generally found the dashboard to have good usability. Our qualitative data (*see Section 5.2.2*) supports these findings, with three participants stating that they thought the dashboard was very user-friendly and two participants expressing the same for the overall system. Six participants stated that they would continue using the system, while two more explained they would do so if minor changes were implemented. Additionally, five users stated they would recommend the system, and eight out of nine participants felt that the system was safe. Overall, the majority of participants perceived the dashboard as useful. These findings suggest that tangible privacy controls are positively received and can be a valuable addition to smart home systems.

The balanced distribution between the use of the tangible and the digital interfaces shows that users' preferences are diverse, which is also supported by our qualitative results. Smart home systems should offer both modalities to accommodate a wider range of users and create a balance between the engaging and playful nature of tangible controls and the convenience of digital controls.

6.3. Limitations and Future Work

While our study provides valuable insights into how systems can raise users' privacy awareness and whether users prefer tangible or digital privacy controls, it also has its limitations. This section discusses the key limitations of our study and outlines potential directions for future work.

Due to time constraints and the fact that we were only able to test one household at a time, our study has a relatively low sample size of nine participants, which limits the generalizability of our findings. Each test phase lasted one week, resulting in a total study duration of one month. While an in-the-wild study leads to more natural behavior from participants than a lab study, our findings indicate that the time period was not sufficient for participants to fully understand the system and integrate it into their daily lives. To gain insights about the long term effects the system has on users, it would therefore be beneficial to increase the individual test phases. Another factor that hindered the fully natural interaction with the system was that we were unable to integrate participants' existing smart home devices into our ecosystem due to the short development period. Instead, we chose three sample devices. It might be beneficial to use devices that already exist in households, as participants would already be familiar with them and could focus more on the privacy aspect of the study. Additionally, some participants remarked that they don't consider the device types we used in our study to be privacy-sensitive. This suggests that integrating a broader range of device types could provide further insights for future studies. Because the tangible dashboard is still in a prototype state, we also encountered some mechanical limitations: we found that the pin connections between the dashboard and the proxies were fragile. To address this issue, they should be replaced with an easier-to-use solution like spring-loaded bolt connectors in the future. Although we implemented a key-lock system to help with the alignment of the proxies, some connections did not work as well as others due to the misalignment of some DuPont plugs. The dashboard was overall very thick and heavy and would profit from a smaller form factor that would allow users to hang it to a wall. Despite a lot of positive feedback, our results show that the system is less accessible for users with a low technical affinity. This could be addressed by providing a detailed user guide with step-by-step instructions. In a future iteration of the system we should also implement the most requested features from *Section 5.2.5*, like a sleep mode that dims the proxy displays so the dashboard is less irritating at night or the ability to control devices with the dashboard and show their status.

Overall, we recommend implementing discrete privacy controls for future systems. We found that tangible privacy controls are more engaging for users and that visualization tools can help raise privacy awareness. For future work, a study with more participants, longer test phases, and the integration of previously owned smart home devices could be promising.

7. Conclusion

We presented a tangible smart home dashboard that lets users map out their smart home as a floor plan to provide information about the type and location of smart home devices. The dashboard features a tangible control interface that lets users make individual decisions about their privacy for each connected device. Local mode lets users access their smart home devices only within the same network, with no connections to the outside. Online mode provides access to smart home devices from anywhere via a password-secured service. Online-shared mode additionally allows users to control their devices using third-party hubs. To increase transparency about the data flow in smart home systems, the dashboard visualizes data streams in real-time using LEDs.

This thesis aimed to answer the following research questions: (1) What effect does the system have on the privacy awareness of users? (2) Do users prefer tangible or digital privacy controls? Our findings show that the system raised the users' privacy awareness, with participants stating that it increased their familiarity and knowledge about data protection in smart homes. While the tangible dashboard played a notable role in our findings, it is important to remember that the participants interacted with the system as a whole (including the PrivacyHub *and* the tangible dashboard) and no part of it can be viewed fully isolated. Users showed a balanced preference between tangible and digital privacy controls, with some preferring the convenience of a digital solution, others the engagement of the tangible interface, and some a mixture of both options. Users perceived the dashboard as very usable (mean SUS score = 81.56) and the majority of users thought the system felt safe.

Our study offers several implications for the design of future systems. The rise in privacy awareness for the majority of participants shows that the integration of clear and intuitive visualizations can effectively educate users about privacy-related issues. The balance between the use of tangible and digital privacy controls indicates that future smart home systems should incorporate both modalities to fit a wider range of user needs, ensuring convenience while still being engaging and accessible. While privacy is usually not a high concern for users, there is a clear demand for more accessible privacy management options in smart homes.

For future work we recommend a bigger sample size to validate our findings, a longer study duration to make sure users fully integrate the system into their lives, and a broader range of supported smart home devices, so users can pair their own devices for a more natural interaction.

Bibliography

[1] Tainyi (Ted) Luor, Hsi-Peng Lu, Hueiju Yu, Yinshiu Lu. "Exploring the Critical Quality Attributes and Models of Smart Homes". In: *Maturitas* 82.4 (Dec. 1, 2015), pp. 377–386. ISSN: 0378-5122. DOI: 10.1016/j.maturitas.2015.07.025. URL: https://www.sciencedirect.com/science/article/pii/S0378512215300311 (visited on 06/13/2024).

[2] Luca Hernández Acostsa, Delphine Reinhardt. "Multi-User Privacy with Voice-Controlled Digital Assistants". In: *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events (PerCom Workshops)*. 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events (PerCom Workshops). Mar. 2022, pp. 30–33. DOI: 10.1109/PerComWorkshops53856.2022.9767270. URL: https://ieeexplore.ieee.org/document/9767270 (visited on 06/12/2024).

[3] Imtiaz Ahmad, Taslima Akter, Zachary Buher, Rosta Farzan, Apu Kapadia, Adam J. Lee. "Tangible Privacy for Smart Voice Assistants: Bystanders' Perceptions of Physical Device Controls". In: *Proceedings of the ACM on Human-Computer Interaction* 6 (CSCW2 Nov. 11, 2022), 364:1–364:31. DOI: 10.1145/3555089. URL: https://dl.acm.org/doi/10.1145/3555089 (visited on 06/17/2024).

[4] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, Adam J. Lee. "Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy". In: *Proceedings of the ACM on Human-Computer Interaction* 4 (CSCW2 Oct. 15, 2020), 116:1–116:28. DOI: 10.1145/3415187. URL: https://dl.acm.org/doi/10.1145/3415187 (visited on 04/25/2024).

[5] Wael S Albayaydh, Ivan Flechais. "Exploring Bystanders' Privacy Concerns with Smart Homes in Jordan". In: *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. CHI '22. New York, NY, USA: Association for Computing Machinery, Apr. 29, 2022, pp. 1–24. ISBN: 978-1-4503-9157-3. DOI: 10.1145/3491102.3502097. URL: https://dl.acm.org/doi/10.1145/3491102.3502097 (visited on 06/13/2024).

[6] Frances K. Aldrich. "Smart Homes: Past, Present and Future". In: *Inside the Smart Home*. Ed. by Richard Harper. London: Springer, 2003, pp. 17–39. ISBN: 978-1-85233-854-1. DOI: 10.1007/1-85233-854-7_2. URL: https://doi.org/10.1007/1-85233-854-7_2 (visited on 04/09/2024).

[7] Ahmed Alshehri, Joseph Spielman, Amiya Prasad, Chuan Yue. "Exploring the Privacy Concerns of Bystanders in Smart Homes from the Perspectives of Both Owners and Bystanders". In: *Proceedings on Privacy Enhancing Technologies* (2022). ISSN: 2299-0984. DOI: 10.56553/popets-2022-0064. URL: https://petsymposium.org/popets/2022/popets-2022-0064.php (visited on 06/14/2024).

[8] Mahdi Nasrullah Al-Ameen, Apoorva Chauhan, M. A. Manazir Ahsan, Huzeyfe Kocabas. ""Most Companies Share Whatever They Can to Make Money!": Comparing User's Perceptions with the Data Practices of IoT Devices". In: *Human Aspects of Information Security and Assurance*. Ed. by Nathan Clarke, Steven Furnell. Cham: Springer International Publishing, 2020, pp. 329–340. ISBN: 978-3-030-57404-8. DOI: 10.1007/978-3-030-57404-8_25.

[9] Mahdi Nasrullah Al-Ameen, Apoorva Chauhan, M.A. Manazir Ahsan, Huzeyfe Kocabas. "A Look into User's Privacy Perceptions and Data Practices of IoT Devices". In: *Information & Computer Security* 29.4 (Jan. 1, 2021), pp. 573–588. ISSN: 2056-4961. DOI: 10.1108/ICS-08-2020-0134. URL: https://doi.org/10.1108/ICS-08-2020-0134 (visited on 06/12/2024).

[10] Ioannis Andrea, Chrysostomos Chrysostomou, George Hadjichristofi. "Internet of Things: Security Vulnerabilities and Challenges". In: *2015 IEEE Symposium on Computers and Communication (ISCC)*. 2015 IEEE Symposium on Computers and Communication (ISCC). July 2015, pp. 180–187. DOI: 10.1109/ISCC.2015.7405513. URL: https://ieeexplore.ieee.org/abstract/document/7405513 (visited on 06/05/2024).

[11] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, Yi Zhou. "Understanding the Mirai Botnet". In: 26th USENIX Security Symposium (USENIX Security 17). 2017, pp. 1093–1110. ISBN: 978-1-931971-40-9. URL: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis (visited on 06/07/2024).

[12] Aaron Bangor, Philip Kortum, James Miller. "Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale". In: *J. Usability Studies* 4.3 (May 1, 2009), pp. 114–123.

[13] Julia Bernd, Ruba Abu-Salma, Alisa Frik. "Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance". In: 10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20). 2020. URL: https://www.usenix.org/conference/foci20/presentation/bernd (visited on 06/17/2024).

[14] Matt Day Bloomberg Giles Turner and Natalia Drozdiak /. *Thousands of Amazon Workers Listen to Alexa Users' Conversations*. TIME. Apr. 11, 2019. URL: https://time.com/5568815/amazon-workers-listen-to-alexa/ (visited on 06/07/2024).

[15] Dieter Bohn. *Exclusive: Amazon Says 100 Million Alexa Devices Have Been Sold*. The Verge. Jan. 4, 2019. URL: https://www.theverge.com/2019/1/4/18168565/amazon-alexa-devices-how-many-sold-number-100-million-dave-limp (visited on 06/07/2024).

[16] John Brooke. "SUS: A 'Quick and Dirty' Usability Scale". In: *Usability Evaluation In Industry*. CRC Press, 1996. ISBN: 978-0-429-15701-1.

[17] Sara Cannizzaro, Rob Procter, Sinong Ma, Carsten Maple. "Trust in the Smart Home: Findings from a Nationally Representative Survey in the UK". In: *PLOS ONE* 15.5 (May 29, 2020), e0231615. ISSN: 1932-6203. DOI: 10.1371/journal.pone.0231615. URL: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0231615 (visited on 06/13/2024).

[18] Peng Cheng, Utz Roedig. "Personal Voice Assistant Security and Privacy—A Survey". In: *Proceedings of the IEEE* 110.4 (Apr. 2022), pp. 476–507. ISSN: 1558-2256. DOI: 10.1109/JPROC.2022.3153167. URL: https://ieeexplore.ieee.org/abstract/document/9733178 (visited on 06/07/2024).

[19] Camille Cobb, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, Lujo Bauer. ""I Would Have to Evaluate Their Objections": Privacy Tensions between Smart Home Device Owners and Incidental Users". In: *Proceedings on Privacy Enhancing Technologies* (2021). ISSN: 2299-0984. DOI: 10.2478/popets-2021-0060. URL: https://petsymposium.org/popets/2021/popets-2021-0060.php (visited on 06/16/2024).

[20] Sarah Delgado Rodriguez, Priyasha Chatterjee, Anh Dao Phuong, Florian Alt, Karola Marky. "Do You Need to Touch? Exploring Correlations between Personal Attributes and Preferences for Tangible Privacy Mechanisms". In: *Proceedings of the CHI Conference on Human Factors in Computing Systems*. CHI '24. New York, NY, USA: Association for Computing Machinery, May 11, 2024, pp. 1–23. ISBN: 9798400703300. DOI: 10.1145/3613904.3642863. URL: https://doi.org/10.1145/3613904.3642863 (visited on 07/23/2024).

[21] Sarah Delgado Rodriguez, Sarah Prange, Christina Vergara Ossenberg, Markus Henkel, Florian Alt, Karola Marky. "PriKey – Investigating Tangible Privacy Control for Smart Home Inhabitants and Visitors". In: *Nordic Human-Computer Interaction Conference*. NordiCHI '22. New York, NY, USA: Association for Computing Machinery, Oct. 8, 2022, pp. 1–13. ISBN: 978-1-4503-9699-8. DOI: 10.1145/3546155.3546640. URL: https://dl.acm.org/doi/10.1145/3546155.3546640 (visited on 04/25/2024).

[22] Youngwook Do, Jung Wook Park, Yuxi Wu, Avinandan Basu, Dingtian Zhang, Gregory D. Abowd, Sauvik Das. "Smart Webcam Cover: Exploring the Design of an Intelligent Webcam Cover to Improve Usability and Trust". In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5.4 (Dec. 30, 2022), 154:1–154:21. DOI: 10.1145/3494983. URL: https://dl.acm.org/doi/10.1145/3494983 (visited on 06/18/2024).

[23] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, Lorrie Faith Cranor. "Exploring How Privacy and Security Factor into IoT Device Purchase Behavior". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. CHI '19. New York, NY, USA: Association for Computing Machinery, May 2, 2019, pp. 1–12. ISBN: 978-1-4503-5970-2. DOI: 10.1145/3290605.3300764. URL: https://dl.acm.org/doi/10.1145/3290605.3300764 (visited on 06/12/2024).

[24] Sebastian S. Feger, Maximiliane Windl, Jesse Grootjen, Albrecht Schmidt. "ConnectivityControl: Providing Smart Home Users with Real Privacy Configuration Options". In: *End-User Development*. Ed. by Lucio Davide Spano, Albrecht Schmidt, Carmen Santoro, Simone Stumpf. Cham: Springer Nature Switzerland, 2023, pp. 180–188. ISBN: 978-3-031-34433-6. DOI: 10.1007/978-3-031-34433-6_11.

[25] Thomas Franke, Christiane Attig, Daniel Wessel. "A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale". In: *International Journal of Human–Computer Interaction* 35.6 (Apr. 3, 2019), pp. 456–467. ISSN: 1044-7318. DOI: 10.1080/10447318.2018.1456150. URL: https://doi.org/10.1080/10447318.2018.1456150 (visited on 06/14/2024).

[26] Christine Geeng, Franziska Roesner. "Who's In Control? Interactions In Multi-User Smart Homes". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. CHI '19. New York, NY, USA: Association for Computing Machinery, May 2, 2019, pp. 1–13. ISBN: 978-1-4503-5970-2. DOI: 10.1145/3290605.3300498. URL: https://dl.acm.org/doi/10.1145/3290605.3300498 (visited on 06/17/2024).

[27] Nina Gerber, Benjamin Reinheimer, Melanie Volkamer. "Home Sweet Home? Investigating Users' Awareness of Smart Home Privacy Threats". In: *Proceedings of An Interactive Workshop on the Human aspects of Smarthome Security and Privacy (WSSP), Baltimore, MD, August 12, 2018* (2018). DOI: 10.5445/IR/1000083578. URL: https://publikationen.bibliothek.kit.edu/1000083578 (visited on 05/30/2024).

[28] Gunnar Harboe, Elaine M. Huang. "Real-World Affinity Diagramming Practices: Bridging the Paper-Digital Gap". In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. CHI '15. New York, NY, USA: Association for Computing Machinery, Apr. 18, 2015, pp. 95–104. ISBN: 978-1-4503-3145-6. DOI: 10.1145/2702123.2702561. URL: https://doi.org/10.1145/2702123.2702561 (visited on 07/05/2024).

[29] Jason Hong. "The Privacy Landscape of Pervasive Computing". In: *IEEE Pervasive Computing* 16.3 (2017), pp. 40–48. ISSN: 1558-2590. DOI: 10.1109/MPRV.2017.2940957. URL: https://ieeexplore.ieee.org/abstract/document/7994573 (visited on 05/31/2024).

[30] Haojian Jin, Boyuan Guo, Rituparna Roychoudhury, Yaxing Yao, Swarun Kumar, Yuvraj Agarwal, Jason I. Hong. "Exploring the Needs of Users for Supporting Privacy-Protective Behaviors in Smart Homes". In: *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. CHI '22. New York, NY, USA: Association for Computing Machinery, Apr. 29, 2022, pp. 1–19. ISBN: 978-1-4503-9157-3. DOI: 10.1145/3491102.3517602. URL: https://dl.acm.org/doi/10.1145/3491102.3517602 (visited on 06/07/2024).

[31] Haojian Jin, Gram Liu, David Hwang, Swarun Kumar, Yuvraj Agarwal, Jason I. Hong. *Peekaboo: A Hub-Based Approach to Enable Transparency in Data Processing within Smart Homes (Extended Technical Report)*. May 18, 2022. DOI: 10.48550/arXiv.2204.04540. arXiv: 2204.04540 [cs]. URL: http://arxiv.org/abs/2204.04540 (visited on 06/18/2024). Pre-published.

[32] Nickson M. Karie, Nor Masri Sahri, Wencheng Yang, Craig Valli, Victor R. Kebande. "A Review of Security Standards and Frameworks for IoT-Based Smart Environments". In: *IEEE Access* 9 (2021), pp. 121975–121995. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3109886. URL: https://ieeexplore.ieee.org/abstract/document/9528421 (visited on 06/07/2024).

[33] Jane E. Klobas, Tanya McGill, Xuequn Wang. "How Perceived Security Risk Affects Intention to Use Smart Home Devices: A Reasoned Action Explanation". In: *Computers & Security* 87 (Nov. 1, 2019), p. 101571. ISSN: 0167-4048. DOI: 10.1016/j.cose.2019.101571. URL: https://www.sciencedirect.com/science/article/pii/S0167404819301348 (visited on 05/30/2024).

[34] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, Karrie Karahalios. ""We Just Use What They Give Us": Understanding Passenger User Perspectives in Smart Homes". In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. CHI '21. New York, NY, USA: Association for Computing Machinery, May 7, 2021, pp. 1–14. ISBN: 978-1-4503-8096-6. DOI: 10.1145/3411764.3445598. URL: https://dl.acm.org/doi/10.1145/3411764.3445598 (visited on 06/14/2024).

[35] Oksana Kulyk, Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Nina Gerber, Melanie Volkamer. "Security and Privacy Awareness in Smart Environments – A Cross-Country Investigation". In: *Financial Cryptography and Data Security*. Ed. by Matthew Bernhard, Andrea Bracciali, L. Jean Camp, Shin'ichiro Matsuo, Alana Maurushat, Peter B. Rønne, Massimiliano Sala. Cham: Springer International Publishing, 2020, pp. 84–101. ISBN: 978-3-030-54455-3. DOI: 10.1007/978-3-030-54455-3_7.

[36] Josephine Lau, Benjamin Zimmerman, 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 Nov. 1, 2018), 102:1–102:31. DOI: 10.1145/3274371. URL: https://dl.acm.org/doi/10.1145/3274371 (visited on 06/14/2024).

[37] Euijong Lee, Young-Duk Seo, Se-Ra Oh, Young-Gab Kim. "A Survey on Standards for Interoperability and Security in the Internet of Things". In: *IEEE Communications Surveys & Tutorials* 23.2 (2021), pp. 1020–1047. ISSN: 1553-877X. DOI: 10.1109/COMST.2021.3067354. URL: https://ieeexplore.ieee.org/abstract/document/9381989 (visited on 06/07/2024).

[38] Roxanne Leitão. "Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse". In: *Proceedings of the 2019 on Designing Interactive Systems Conference*. DIS '19. New York, NY, USA: Association for Computing Machinery, June 18, 2019, pp. 527–539. ISBN: 978-1-4503-5850-7. DOI: 10.1145/3322276.3322366. URL: https://dl.acm.org/doi/10.1145/3322276.3322366 (visited on 06/19/2024).

[39] Jinyang Li, Zhenyu Li, Gareth Tyson, Gaogang Xie. "Characterising Usage Patterns and Privacy Risks of a Home Security Camera Service". In: *IEEE Transactions on Mobile Computing* 21.7 (July 2022), pp. 2344–2357. ISSN: 1558-0660. DOI: 10.1109/TMC.2020.3039787. URL: https://ieeexplore.ieee.org/document/9266572 (visited on 06/20/2024).

[40] Yanyan Lit, Sara Kim, Eric Sy. "A Survey on Amazon Alexa Attack Surfaces". In: *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*. 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC). Jan. 2021, pp. 1–7. DOI: 10.1109/CCNC49032.2021.9369553. URL: https://ieeexplore.ieee.org/abstract/document/9369553 (visited on 06/07/2024).

[41] Knud Lasse Lueth. *State of the IoT 2018: Number of IoT Devices Now at 7B – Market Accelerating*. IoT Analytics. Aug. 8, 2018. URL: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/ (visited on 06/05/2024).

[42] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, David Wagner. "Privacy Attitudes of Smart Speaker Users". In: *Proceedings on Privacy Enhancing Technologies* 2019.4 (Oct. 2019). DOI: 10.2478/popets-2019-0068. URL: https://par.nsf.gov/biblio/10109137-privacy-attitudes-smart-speaker-users (visited on 06/11/2024).

[43] Shrirang Mare, Franziska Roesner, Tadayoshi Kohno. "Smart Devices in Airbnbs: Considering Privacy and Security for Both Guests and Hosts". In: *Proceedings on Privacy Enhancing Technologies* (2020). ISSN: 2299-0984. DOI: 10.2478/popets-2020-0035. URL: https://petsymposium.org/popets/2020/popets-2020-0035.php (visited on 06/17/2024).

[44] Ibrahim Mashal, Ahmed Shuhaiber. "What Makes Jordanian Residents Buy Smart Home Devices? A Factorial Investigation Using PLS-SEM". In: *Kybernetes* 48.8 (Jan. 1, 2018), pp. 1681–1698. ISSN: 0368-492X. DOI: 10.1108/K-01-2018-0008. URL: https://doi.org/10.1108/K-01-2018-0008 (visited on 06/13/2024).

[45] Aleecia M. McDonald, Robert W. Reeder, Patrick Gage Kelley, Lorrie Faith Cranor. "A Comparative Study of Online Privacy Policies and Formats". In: *Privacy Enhancing Technologies*. Ed. by Ian Goldberg, Mikhail J. Atallah. Berlin, Heidelberg: Springer, 2009, pp. 37–55. ISBN: 978-3-642-03168-7. DOI: 10.1007/978-3-642-03168-7_3.

[46] Vikram Mehta. "Tangible Interactions for Privacy Management". In: *Proceedings of the Thirteenth International Conference on Tangible, Embedded, and Embodied Interaction*. TEI '19. New York, NY, USA: Association for Computing Machinery, Mar. 17, 2019, pp. 723–726. ISBN: 978-1-4503-6196-5. DOI: 10.1145/3294109.3302934. URL: https://dl.acm.org/doi/10.1145/3294109.3302934 (visited on 06/18/2024).

[47] Andrés Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, David Irwin. "Private Memoirs of a Smart Meter". In: *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*. BuildSys '10. New York, NY, USA: Association for Computing Machinery, Nov. 2, 2010, pp. 61–66. ISBN: 978-1-4503-0458-0. DOI: 10.1145/1878431.1878446. URL: https://dl.acm.org/doi/10.1145/1878431.1878446 (visited on 05/27/2024).

[48] David Müller. "Development and Evaluation of a Smart Home Privacy Hub". This thesis represents the counterpart to the tangible dashboard.

[49] Jonathan A. Obar, Anne Oeldorf-Hirsch. "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services". In: *Information, Communication & Society* 23.1 (Jan. 2, 2020), pp. 128–147. ISSN: 1369-118X. DOI: 10.1080/1369118X.2018.1486870. URL: https://doi.org/10.1080/1369118X.2018.1486870 (visited on 06/11/2024).

[50] Joel R. Reidenberg, Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James T. Graves, Fei Liu, Aleecia McDonald, Thomas B. Norton, Rohan Ramanath, N. Cameron Russell, Norman Sadeh, Florian Schaub. "Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding". In: *Berkeley Technology Law Journal* 30 (2015), p. 39. URL: https://heinonline.org/HOL/Page?handle=hein.journals/berktech30&id=51&div=&collection=.

[51] Said Jawad Saidi, Anna Maria Mandalari, Hamed Haddadi, Daniel J. Dubois, David Choffnes, Georgios Smaragdakis, Anja Feldmann. "Detecting Consumer IoT Devices through the Lens of an ISP". In: *Proceedings of the Applied Networking Research Workshop*. ANRW '21. New York, NY, USA: Association for Computing Machinery, July 24, 2021, pp. 36–38. ISBN: 978-1-4503-8618-0. DOI: 10.1145/3472305.3472885. URL: https://dl.acm.org/doi/10.1145/3472305.3472885 (visited on 06/10/2024).

[52] Annika Sabrina Schulz, Johanna Müller, Frank Beruscha. "Experience by Cohabitation: Living in a Smart Home Initiated by Your Partner". In: *Human-Computer Interaction – INTERACT 2023*. Ed. by José Abdelnour Nocera, Marta Kristín Lárusdóttir, Helen Petrie, Antonio Piccinno, Marco Winckler. Cham: Springer Nature Switzerland, 2023, pp. 304–323. ISBN: 978-3-031-42286-7. DOI: 10.1007/978-3-031-42286-7_17.

[53] Anna Kornfeld Simpson, Franziska Roesner, Tadayoshi Kohno. "Securing Vulnerable Home IoT Devices with an In-Hub Security Manager". In: *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). Mar. 2017, pp. 551–556. DOI: 10.1109/PERCOMW.2017.7917622. URL: https://ieeexplore.ieee.org/abstract/document/7917622 (visited on 06/18/2024).

[54] Madiha Tabassum, Tomasz Kosinski, 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, pp. 435–450. ISBN: 978-1-939133-05-2. URL: https://www.usenix.org/conference/soups2019/presentation/tabassum (visited on 05/30/2024).

[55] Parth Kirankumar Thakkar, Shijing He, Shiyu Xu, Danny Yuxing Huang, Yaxing Yao. ""It Would Probably Turn into a Social Faux-Pas": Users' and Bystanders' Preferences of Privacy Awareness Mechanisms in Smart Homes". In: *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. CHI '22. New York, NY, USA: Association for Computing Machinery, Apr. 29, 2022, pp. 1–13. ISBN: 978-1-4503-9157-3. DOI: 10.1145/3491102.3502137. URL: https://dl.acm.org/doi/10.1145/3491102.3502137 (visited on 06/16/2024).

[56] Philipp Thalhammer, David Müller, Alexander Schmidt, Michael Huber, Albrecht Schmidt, Sebastian Feger. "ConnectivityControl: A Model Ecosystem for Advanced Smart Home Privacy". In: *Proceedings of the 22nd International Conference on Mobile and Ubiquitous Multimedia*. MUM '23. New York, NY, USA: Association for Computing Machinery, Dec. 3, 2023, pp. 556–558. ISBN: 9798400709210. DOI: 10.1145/3626705.3631876. URL: https://dl.acm.org/doi/10.1145/3626705.3631876 (visited on 04/09/2024).

[57] Manesh Thankappan, Helena Rifà-Pous, Carles Garrigues. "Multi-Channel Man-in-the-Middle Attacks against Protected Wi-Fi Networks: A State of the Art Review". In: *Expert Systems with Applications* 210 (Dec. 30, 2022), p. 118401. ISSN: 0957-4174. DOI: 10.1016/j.eswa.2022.118401. URL: https://www.sciencedirect.com/science/article/pii/S0957417422015093 (visited on 06/05/2024).

[58] Xuequn Wang, Tanya Jane McGill, Jane E. Klobas. "I Want It Anyway: Consumer Perceptions of Smart Home Devices". In: *Journal of Computer Information Systems* 60.5 (Sept. 2, 2020), pp. 437–447. ISSN: 0887-4417. DOI: 10.1080/08874417.2018.1528486. URL: https://doi.org/10.1080/08874417.2018.1528486 (visited on 06/11/2024).

[59] Maximiliane Windl, Alexander Hiesinger, Robin Welsch, Albrecht Schmidt, Sebastian S. Feger. "SaferHome: Interactive Physical and Digital Smart Home Dashboards for Communicating Privacy Assessments to Owners and Bystanders". In: *Proceedings of the ACM on Human-Computer Interaction* 6 (ISS 2022), pp. 680–699. ISSN: 2573-0142. DOI: 10.1145/3567739. URL: https://research.aalto.fi/en/publications/saferhome-interactive-physical-and-digital-smart-home-dashboards- (visited on 06/03/2024).

[60] Maximiliane Windl, Albrecht Schmidt, Sebastian S. Feger. "Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes". In: *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. CHI '23. New York, NY, USA: Association for Computing Machinery, Apr. 19, 2023, pp. 1–16. ISBN: 978-1-4503-9421-5. DOI: 10.1145/3544548.3581167. URL: https://dl.acm.org/doi/10.1145/3544548.3581167 (visited on 04/25/2024).

[61] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, Yang Wang. "Privacy Perceptions and Designs of Bystanders in Smart Homes". In: *Proceedings of the ACM on Human-Computer Interaction* 3 (CSCW Nov. 7, 2019), 59:1–59:24. DOI: 10.1145/3359161. URL: https://dl.acm.org/doi/10.1145/3359161 (visited on 06/01/2024).

[62] Eric Zeng, Shrirang Mare, 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. ISBN: 978-1-931971-39-3. URL: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng (visited on 06/12/2024).

[63] Serena Zheng, Noah Apthorpe, Marshini Chetty, Nick Feamster. “User Perceptions of Smart Home IoT Privacy”. In: *Proceedings of the ACM on Human-Computer Interaction* 2 (CSCW Nov. 1, 2018), 200:1–200:20. DOI: 10.1145/3274469. URL: https://dl.acm.org/doi/10.1145/3274469 (visited on 06/12/2024).

All links were last followed on July 24, 2024.

A. Questionnaires

This section contains the material that was used in the study, including the questionnaires from before and after the study as well as the interview questions. For easier navigation, all questions were numbered.

Fragebogen (Intro)

Teilnehmer ID: _____

Alter:

Geschlecht:

Beruf / Tätigkeit:

Höchster erreichter Bildungsgrad:

Anzahl der Smart Home Geräte im Haushalt:

1.0 Nutzertyp

Pilot-Nutzer

Ein Benutzer, der die Verantwortung für die Installation von Geräten im Haus trägt, deren Konfiguration übernimmt und die Geräte regelmäßig im Alltag nutzt.

Passagier-Nutzer

Ein Nutzer, dessen tägliches Leben von intelligenten Geräten in seinem Haus beeinflusst wird (entweder durch die eigene Nutzung oder durch die Nutzung einer anderen Person), der aber die Geräte selbst nicht eingerichtet hat oder sie konfiguriert.

Bitte geben Sie an welcher Nutzertyp auf **Sie** zutrifft:

☐ Pilot-Nutzer ☐ Passagier-Nutzer

	Bitte geben Sie den Grad Ihrer **Zustimmung** zu folgenden Aussagen an.	stimmt gar nicht	stimmt weit-gehend nicht	stimmt eher nicht	stimmt eher	stimmt weit-gehend	stimmt völlig
1.1	Ich bin mit Smart Home Systemen sehr vertraut.	☐	☐	☐	☐	☐	☐
1.2	Mir ist Datenschutz sehr wichtig.	☐	☐	☐	☐	☐	☐
1.3	Bei Smart Home Geräten ist mir der Feature-Umfang am wichtigsten.	☐	☐	☐	☐	☐	☐
1.4	Bei Smart Home Geräten ist mir Datenschutz am wichtigsten.	☐	☐	☐	☐	☐	☐
1.5	Ich habe das Gefühl, dass ich Kontrolle über meine privaten Daten in meinem Smart Home habe.	☐	☐	☐	☐	☐	☐
1.6	Ich bin sehr besorgt um meine privaten Daten in meinem Smart Home.	☐	☐	☐	☐	☐	☐
1.7	Ich weiß wie ich meine privaten Daten im Smart Home schützen kann.	☐	☐	☐	☐	☐	☐
1.8	Ich habe das Gefühl, dass ich gut darüber Bescheid weiß was mit meinen privaten Daten in meinem Smart Home passiert.	☐	☐	☐	☐	☐	☐
1.9	Ich beschäftige mich gern genauer mit technischen Systemen.	☐	☐	☐	☐	☐	☐
1.10	Ich probiere gern die Funktionen neuer technischer Systeme aus.	☐	☐	☐	☐	☐	☐
1.11	In erster Linie beschäftige ich mich mit technischen Systemen, weil ich muss.	☐	☐	☐	☐	☐	☐
1.12	Wenn ich ein neues technisches System vor mir habe, probiere ich es intensiv aus.	☐	☐	☐	☐	☐	☐
1.13	Ich verbringe sehr gern Zeit mit dem Kennenlernen eines neuen technischen Systems.	☐	☐	☐	☐	☐	☐

	Bitte geben Sie den Grad Ihrer **Zustimmung** zu folgenden Aussagen an.	stimmt gar nicht	stimmt weit-gehend nicht	stimmt eher nicht	stimmt eher	stimmt weit-gehend	stimmt völlig
1.14	Es genügt mir, dass ein technisches System funktioniert, mir ist es egal, wie oder warum.	☐	☐	☐	☐	☐	☐
1.15	Ich versuche zu verstehen, wie ein technisches System genau funktioniert.	☐	☐	☐	☐	☐	☐
1.16	Es genügt mir, die Grundfunktionen eines technischen Systems zu kennen.	☐	☐	☐	☐	☐	☐
1.17	Ich versuche, die Möglichkeiten eines technischen Systems vollständig auszunutzen.	☐	☐	☐	☐	☐	☐

	Bitte geben Sie an, was für Sie **am ehesten** zutrifft.	mehrmals täglich	einmal täglich	mehrmals die Woche	einmal die Woche	mehrmals im Monat	nie
1.18	Wie oft nutzen Sie Smart Home Geräte?	☐	☐	☐	☐	☐	☐

Fragebogen (Outro)

Teilnehmer ID: _____

	Bitte geben Sie den Grad Ihrer **Zustimmung** zu folgenden Aussagen an.	stimmt gar nicht	stimmt weit-gehend nicht	stimmt eher nicht	stimmt eher	stimmt weit-gehend	stimmt völlig
2.1	Ich bin mit Smart Home Systemen sehr vertraut.	☐	☐	☐	☐	☐	☐
2.2	Mir ist Datenschutz sehr wichtig.	☐	☐	☐	☐	☐	☐
2.3	Bei Smart Home Geräten ist mir der Feature-Umfang am wichtigsten.	☐	☐	☐	☐	☐	☐
2.4	Bei Smart Home Geräten ist mir Datenschutz am wichtigsten.	☐	☐	☐	☐	☐	☐
2.5	Ich habe das Gefühl, dass ich Kontrolle über meine privaten Daten in meinem Smart Home habe.	☐	☐	☐	☐	☐	☐
2.6	Ich bin sehr besorgt um meine privaten Daten in meinem Smart Home.	☐	☐	☐	☐	☐	☐
2.7	Ich weiß wie ich meine privaten Daten im Smart Home schützen kann.	☐	☐	☐	☐	☐	☐
2.8	Ich habe das Gefühl, dass ich gut darüber Bescheid weiß was mit meinen privaten Daten in meinem Smart Home passiert.	☐	☐	☐	☐	☐	☐

Privacy Hub

	Bitte geben Sie den Grad Ihrer **Zustimmung** zu folgenden Aussagen an.	Stimme überhaupt nicht zu				Stimme voll zu
3.1	Ich denke, dass ich das System gerne häufig benutzen würde.	☐	☐	☐	☐	☐
3.2	Ich fand das System unnötig komplex.	☐	☐	☐	☐	☐
3.3	Ich fand das System einfach zu benutzen.	☐	☐	☐	☐	☐
3.4	Ich glaube, ich würde die Hilfe einer technisch versierten Person benötigen, um das System benutzen zu können.	☐	☐	☐	☐	☐
3.5	Ich fand, die verschiedenen Funktionen in diesem System waren gut integriert.	☐	☐	☐	☐	☐
3.6	Ich denke, das System enthält zu viele Inkonsistenzen.	☐	☐	☐	☐	☐
3.7	Ich kann mir vorstellen, dass die meisten Menschen den Umgang mit diesem System sehr schnell lernen.	☐	☐	☐	☐	☐
3.8	Ich fand das System sehr umständlich zu nutzen.	☐	☐	☐	☐	☐
3.9	Ich fühlte mich bei der Benutzung des Systems sehr sicher.	☐	☐	☐	☐	☐
3.10	Ich musste eine Menge lernen, bevor ich anfangen konnte, das System zu verwenden.	☐	☐	☐	☐	☐

Physisches Dashboard

	Bitte geben Sie den Grad Ihrer **Zustimmung** zu folgenden Aussagen an.	Stimme überhaupt nicht zu				Stimme voll zu
3.1	Ich denke, dass ich das System gerne häufig benutzen würde.	☐	☐	☐	☐	☐
3.2	Ich fand das System unnötig komplex.	☐	☐	☐	☐	☐
3.3	Ich fand das System einfach zu benutzen.	☐	☐	☐	☐	☐
3.4	Ich glaube, ich würde die Hilfe einer technisch versierten Person benötigen, um das System benutzen zu können.	☐	☐	☐	☐	☐
3.5	Ich fand, die verschiedenen Funktionen in diesem System waren gut integriert.	☐	☐	☐	☐	☐
3.6	Ich denke, das System enthält zu viele Inkonsistenzen.	☐	☐	☐	☐	☐
3.7	Ich kann mir vorstellen, dass die meisten Menschen den Umgang mit diesem System sehr schnell lernen.	☐	☐	☐	☐	☐
3.8	Ich fand das System sehr umständlich zu nutzen.	☐	☐	☐	☐	☐
3.9	Ich fühlte mich bei der Benutzung des Systems sehr sicher.	☐	☐	☐	☐	☐
3.10	Ich musste eine Menge lernen, bevor ich anfangen konnte, das System zu verwenden.	☐	☐	☐	☐	☐

Folge Interview

Allgemein

5.1 Welches Feature des Systems haben Sie am meisten genutzt?

5.2 Wann haben Sie Änderungen an den Privacy States vorgenommen? Warum?

5.3 Wie intuitiv war es für Sie, Privacy States für verschiedene Geräte festzulegen? Warum?

5.4 Wo haben Sie die Privacy States überwiegend eingestellt? Warum?

5.5 Wie hat sich Ihr Bewusstsein/Ihre Haltung zu Privacy durch die Interaktion mit dem System verändert?

5.6 Würden Sie das System auch privat nutzen? Warum? Welche Teile davon?

5.7 Würden Sie das System Ihren Freunden oder Ihrer Familie empfehlen? Warum oder warum nicht?

5.8 Hatten Sie irgendwelche Probleme bei der Nutzung des Systems? Wenn ja, welche?

5.9 Wie sicher (im Bezug auf Privacy) haben Sie sich beim Einsatz des Systems gefühlt?

5.10 Welche zusätzlichen Features würden Sie sich für das System wünschen?

5.11 Wie hat das System Ihnen geholfen, bessere Entscheidungen über den Datenschutz in Ihrem Smart Home zu treffen?

Hub

5.12 Wie haben Sie die Interaktion mit den Websites empfunden?

5.13 Wie haben Sie die Visualisierungen des LED-Rings empfunden? Warum?

5.14 Wann haben Sie die Online Website genutzt und warum?

5.15 Welche Einblicke haben Sie durch die History bekommen?

5.16 Haben Sie einen Third Party Hub mit dem System verbunden? Was waren Ihre Erfahrungen mit diesem Feature?

5.17 Was würden Sie am Hub verbessern?

Dashboard

5.18 Wie haben Sie die haptische Interaktion mit dem System empfunden? Finden Sie eine haptische oder eine rein digitale Experience angenehmer? Oder eine Mischung aus beidem?

5.19 Wie haben Sie die visuelle Darstellung der Datenflüsse auf dem Dashboard empfunden?

5.20 Wie haben sich die Visualisierungen der Datenflüsse auf dem Dashboard auf ihre Wahrnehmung bezüglich Privacy ausgewirkt?

5.21 Wie hilfreich war das Dashboard bei der Verwaltung und Überwachung Ihres Smart Home?

5.22 Was würden Sie am Dashboard verbessern?

5.23 Haben Sie sonst noch irgendwelche Anmerkungen?