Windl, Maximiliane; Hiesinger, Alexander; Welsch, Robin; Schmidt, Albrecht; Feger, Sebastian S.

SaferHome: Interactive Physical and Digital Smart Home Dashboards for Communicating Privacy Assessments to Owners and Bystanders

Published in:
Proceedings of the ACM on Human-Computer Interaction

DOI:
10.1145/3567739

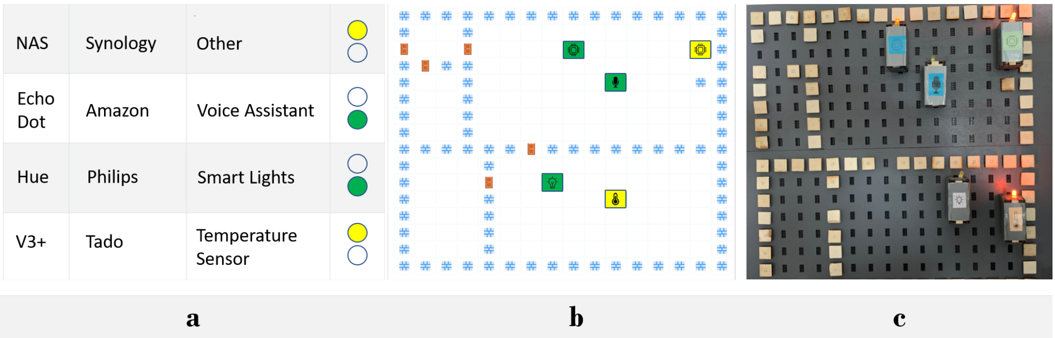
Published: 01/01/2022

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Please cite the original version:
Windl, M., Hiesinger, A., Welsch, R., Schmidt, A., & Feger, S. S. (2022). SaferHome: Interactive Physical and Digital Smart Home Dashboards for Communicating Privacy Assessments to Owners and Bystanders. *Proceedings of the ACM on Human-Computer Interaction*, *6*(ISS), 680-699. https://doi.org/10.1145/3567739

SaferHome: Interactive Physical and Digital Smart Home Dashboards for Communicating Privacy Assessments to Owners and Bystanders

MAXIMILIANE WINDL, LMU Munich, Germany and Munich Center for Machine Learning, Germany
ALEXANDER HIESINGER, LMU Munich, Germany
ROBIN WELSCH, Aalto University, Finland
ALBRECHT SCHMIDT, LMU Munich, Germany
SEBASTIAN S. FEGER, LMU Munich, Germany



NAS	Synology	Other	🟡 ○
Echo Dot	Amazon	Voice Assistant	○ 🟢
Hue	Philips	Smart Lights	○ 🟢
V3+	Tado	Temperature Sensor	🟡 ○

Fig. 1. Overview of SaferHome's three device views: **a) digital list view** that uses two state traffic lights as metaphors to communicate threat assessments, and **b) a digital** and **c) a functional physical dashboard**, both customized according to the smart homes' floor plans and device locations.

Private homes are increasingly becoming smart spaces. While smart homes promise comfort, they expose most intimate spaces to security and privacy risks. Unfortunately, most users today are not equipped with the right tools to assess the vulnerabilities or privacy practices of smart devices. Further, users might lose track of the devices installed in their homes or are unaware of devices placed by a partner or host. We developed SaferHome, an interactive digital-physical privacy framework, to provide smart home users with security and privacy assessments and a sense of device location. SaferHome includes a digital list view and physical and digital dashboards that map real floor plans. We evaluated SaferHome with eight households in the wild. We find that users adopted various strategies to integrate the dashboards into their understanding and interpretation of smart home privacy. We present implications for the design of future smart home privacy frameworks that are impacted by technical affinity, device types, device ownership, and tangibility of assessments.

Authors' addresses: Maximiliane Windl, LMU Munich, Munich, Germany and Munich Center for Machine Learning, Munich, Germany, maximiliane.windl@ifi.lmu.de; Alexander Hiesinger, LMU Munich, Munich, Germany, alexander.hiesinger@campus.lmu.de; Robin Welsch, Aalto University, Espoo, Finland, robin.welsch@aalto.fi; Albrecht Schmidt, LMU Munich, Frauenlobstr. 7a, Munich, Germany, albrecht.schmidt@ifi.lmu.de; Sebastian S. Feger, LMU Munich, Frauenlobstr. 7a, Munich, Germany, sebastian.feger@ifi.lmu.de.

CCS Concepts: • **Security and privacy → Usability in security and privacy**; • **Human-centered computing → Empirical studies in HCI**.

Additional Key Words and Phrases: IoT, smart home, privacy, security, physical and digital interactive dashboards, bystander privacy.

ACM Reference Format:
Maximiliane Windl, Alexander Hiesinger, Robin Welsch, Albrecht Schmidt, and Sebastian S. Feger. 2022. SaferHome: Interactive Physical and Digital Smart Home Dashboards for Communicating Privacy Assessments to Owners and Bystanders. *Proc. ACM Hum.-Comput. Interact.* 6, ISS, Article 586 (December 2022), 20 pages. https://doi.org/10.1145/3567739

1 INTRODUCTION

Connected devices are becoming ubiquitous in many households. Devices like voice assistants, connected light bulbs, and smart televisions promise comfort and entertainment and are therefore increasingly connected to home networks [19, 22]. The downside: such network devices, also referred to as the Internet of Things (IoT) devices, might expose users and their intimate data to various security and privacy threats [34]. Reasons for this include fast development cycles, manufacturers not following IoT standards (e.g., ENISA [14, 15]), and privacy violations by design.

Potential threats to smart home users are manifold. Data misuse can happen *by design*, in case manufacturers employ dubious business models or fail to inform users of how they use data recorded in their most intimate spaces. Examples include smart televisions that record and transmit camera and usage data [2, 21], voice assistants recording home conversations that human analysts might listen to [5, 16], and manufacturers of robotic vacuum cleaners that sell floor plans to third parties [3]. There are also numerous examples of data breaches in the home that are *unintentional*. Here, attackers make use of hardware or software vulnerabilities that provide access to intimate user data, even of sexual nature [40, 43]. Those are strong examples of how device security links directly to privacy.

Unfortunately, smart home users often report lacking the right tools to make informed decisions about the security and privacy of their devices [10, 13, 33]. This remains true even though computer security and privacy research have advanced in the systematic evaluation of devices [28]. Clearly, the assessment and evaluation of smart devices represent technical and human challenges in the domain of usable security and privacy [7, 18, 37]. Those challenges extend way beyond the privacy of the owner of the smart device. Instead, they also affect everyone living in a multi-user environment with connected devices, independent of their relationship and ability to negotiate with the primary device responsible [20, 44]. In contrast, *visitors* are likely to have even less awareness of smart devices, their location, and abilities, resulting in personal coping strategies and host-visitor negotiations [31, 44].

Not only do smart home users lack evaluation tools, but research has also shown a fundamental mismatch between security and privacy concepts and awareness in users' device assessments [34]. In response, several research initiatives attempt to increase user awareness and aim at empowering users to make informed decisions. Privacy and security labels [12] are expected to communicate crucial information during device selection and purchase but are mostly limited to static information or require users to frequently check for updated information manually. SAFER, in contrast, represents an example of a more dynamic framework that might be used to actively inform users about device updates that benefit their privacy and security [34]. The development of such software frameworks is heavily impacted by research on the visualization of device security and privacy information [23]. Yet, evaluations have generally been limited to short interactions on mock data that do not relate to users' actual devices and configurations.

In contrast, SaferHome enables users to capture the entire configuration of connected devices in their homes and provides initial security and privacy assessments. As depicted in Figure 1, the framework offers three views: a digital list view and two types of dashboards that provide references to actual household floor plans and corresponding device locations, giving users an overview of their devices' contexts of use. We developed digital and physical floor plan dashboards with the same granularity and resolution to evaluate how device context of use impacts users' security and privacy awareness. We evaluated SaferHome and its impact on users' awareness in a mixed-method study involving eight households and 16 participants. Each household first used the digital list view for one week before experiencing either the digital or physical floor plan dashboard for another week, adding up to two weeks of SaferHome usage. We find that systems like SaferHome can help to increase users' awareness of privacy threats and the capabilities of their devices. Further, we find that both interpretations of privacy threats and users' ability to act on recommendations are impacted by their technical affinity and device ownership roles. Our paper makes three key contributions:

- We present SaferHome, a device security and privacy framework that enables users to capture their smart home configurations. In particular, we detail the architectures of our digital and physical dashboards and show how device privacy assessments can be communicated through a tangible interactive surface.
- We report on findings from an in-the-wild study with eight households and 16 participants using SaferHome for two weeks. Two dashboards provided a sense of device context through the representation of actual floor plans.
- Finally, we present research challenges and implications for the design of future smart home privacy frameworks that relate to device ownership, multi-user interactions, users' technical affinity, and the role of interactive tangible artifacts and dashboards for privacy communication and awareness.

2 RELATED WORK

Device security and privacy are essential in connected spaces, particularly in smart homes. Security of devices and networks, often referred to as cyber security, concerns protection against physical damage of hardware, as well as unwanted information disclosure and data theft [38]. As such, device *security* is a fundamental quality and requirement for privacy. Information *privacy* generally refers to individuals' desire to control their data, in particular related to access, sharing, and use [6]. Device security vulnerabilities can compromise access to data stored on the targeted device or devices in the same network, jeopardizing user privacy. But, information privacy is also at risk when service providers intentionally misuse data or record and share them as part of dubious business practices.

2.1 Security and Privacy Awareness

Chalhoub et al. [10] found in a longitudinal in situ study that smart home users have concerns regarding the intrusiveness of cameras and voice-enabled devices, which is in line with findings from Nguyen et al. [33]. Additionally, they found that users perceived a physical camera shutter as more effective than an LED in indicating the active state of features, such as ongoing voice recording. Thus, they recommend physical controls as effective control mechanisms. **Our research follows the authors' in situ approach to capture real configurations and experiences.**

Oser et al. [34] studied how access to security and privacy reports impacts users' awareness and decisions both in a private and enterprise IoT context, before and after device purchase. The authors developed a prototypical platform called SAFER with mock reports on a wide variety of mock devices. Their mixed-method study found that users generally want to consult the framework before device purchase and that this would likely influence their final decision. Yet, the authors also found a mismatch between users' perceptions of security and privacy, occasionally mistaking one for the other. In response, the authors recommended clearly communicating security and privacy reports' background and potential impact on future systems. **This work has inspired our own investigation, transitioning from a mockup to a framework that allows users to store and track real smart home configurations.**

2.2 Threat Assessment and Communication

As cyber security researchers progress towards a more systematic and large-scale identification and analysis of network devices [35], the challenge of presenting the information in an understandable and actionable way to device users grows. In this context, Huang et al. [23] investigated different threat visualizations. They designed an IoT security framework with three presentation modes: risk table, risk map, and risk tree. The risk table is a simple table listing device assets, access methods, and corresponding impacts. The risk map is a formatted table with threats and risks aligned with critical assets based on cell dimension and color-coding. Finally, the risk tree represents critical assets as roots, threats as children, and risks as leaves. They found that the risk map, a list that relies heavily on cell color coding, was preferred by most users as they found it easier to understand. **SaferHome's development profited from these findings, employing color-coding of risk indicators.**

Risk communication was identified as a key challenge in the work of Oser et al. [34]. Their mock framework SAFER offered both a guided and detailed view. However, they did not find a significant difference between the two views regarding tool functionality and helpfulness. Rather, they found that the primary risk indicator, i.e., the traffic light in the guided view and general color coding in the detailed view, informed device risk concern and removal acceptance of users. Additionally, participants mentioned that they generally expected a more binary communication style. **These findings influenced the design of our framework, which is limited to two states: (1) no critical warnings and (2) risk concerns detected. In addition, whenever possible, we provide technical references to risk reports and accessible interpretations, similar to the detailed and guided views on SAFER.**

2.3 Effects of Location and Ownership

Not only the users of smart home devices are exposed to privacy and security threats, but also other household members and visitors. Literature often refers to these people as *bystanders*, i.e., people who are not the primary users of technology but are nevertheless exposed to it [31, 44]. This potential power struggle related to ownership and technology affinity has even caused concerns related to abusive partnerships [27].

But, also in functional partnerships and functional host-guest relationships, multi-user control represents important challenges. Kwon et al. [25] investigated perceptions around interaction and retrospective analysis of intimate data recorded by a connected smart shower. The authors found that the participants did not perceive the data recording as troubling. The informants also did not consider the retrospective exploration of the recorded data as a sensitive process. But, the authors noted that the collaborative sense-making of the data around water usage accountability generated sensitivity. In contrast, Marky et al. [31] investigated privacy perceptions of smart home *visitors*. Their findings showed that visitors cannot effectively protect their privacy in smart houses and are often unaware of being tracked. Further, the authors found that visitors considered their relation to the device owner and familiarity with the smart environment as factors when navigating and interacting with the visited home. Notably, "visitors of smart environments demonstrated similar privacy preferences like the owners of IoT devices but lacked means to judge consequences of data collection and means to express their privacy preferences." Geeng and Roesner [20] classified smart home users as *drivers* and *passive users*. They found that tech-savvy users had increased access and control over device functionality. **Recognizing these important multi-user privacy challenges, we also explored inter-dependencies and attitudes towards technology as part of our study. In particular, we investigated self-reported technology responsibility in the household, aligned with work by Koshy et al. [24], who distinguished between device *pilot* users and *passenger* users.**

Zeng and Roesner [45] also stressed that device access in multi-user environments is not solved. They developed an app that lists devices according to their location in the household, enabling fine-grained access rights to individual devices. The notion of device location in the smart home is also echoed in the work of Chalhoub et al. [10]. They described a connection between the desire for effective privacy measures and device locations. For example, a participant reported that a physical camera shutter provided sufficient assurance to keep a smart device in the bathroom, a very intimate space. Yao et al. [44] further "highlighted bystanders' needs for privacy and control, as well as the tension of privacy expectations between the owners/users and the bystanders in smart homes." They found that some bystanders employ strategies to locate devices and assess their potential impact. **Recognizing this general need to identify existing devices, their operational states, and their location, we developed dashboards that represent actual floor plans and the devices' locations.**

2.4 Security and Privacy Assessment Tools

Related work has shown that users do not currently have the right tools to evaluate the security and privacy of smart devices. Yet, we see an effort toward the development of assistive tools. The app developed by Zeng and Roesner [45] allows defining access to devices in a very detailed manner, thus contributing to multi-user privacy. Emami-Naeini et al. [13] developed privacy and security labels that support users in making informed decisions when purchasing IoT devices. The labels, inspired by nutrition labels, feature information about security and privacy assessments of the device and manufacturer. Notably, the design of the labels has been further improved with the help of security experts, and device users [12].

The SAFER framework allows users to track devices [34]. Users are expected to be informed immediately and automatically about updated privacy and security reports about their registered devices. Their findings highlighted that a framework like SAFER is appreciated in business and private contexts. Yet, the SAFER framework was limited to mock data and mock devices. Accordingly, the interaction of the study participants with the mock data was brief. **In contrast, we developed SaferHome to capture the entire smart home configuration of real households. The sample size of our study aligns closely with the work of Oser et al. [34], as we recruited 16 participants for a between-subjects study. In contrast, our study is not limited to a brief exploration of mock data but represents a longitudinal two-week study.**

2.5 Summary and Research Questions

IoT device users do not currently have the right tools to make informed decisions. Tools focused either on a more static communication of assessments [13] or on interactions with mock devices and mock data [34]. In contrast, we designed SaferHome to support the mapping of real household configurations. Our study participants interacted with the service for two weeks. In the first week, they could review device assessments on a digital list view before experiencing a digital and/or physical interactive smart home dashboard in the second week. This enabled us further to explore effects around device location and multi-user smart homes. Overall, our work addresses the following research questions (RQs):

RQ1: How does SaferHome impact the privacy awareness of smart home users? We designed SaferHome to provide privacy assessments related to actual smart home configurations. This allows us to study how SaferHome impacts the privacy awareness of smart home users and their ability to make informed decisions.

RQ2: How do smart home users experience the interaction with dashboards that map floor plans? Device security and privacy threat visualizations are often based on traditional list views, tables, or representations derived from structured list elements, such as tree views. We recognized that the growing number and diversity of connected devices in smart homes requires visualizations that place devices into their context of use. Therefore, we implemented a physical and digital dashboard that allows users to map their floor plans and device locations. The dashboards feature indicators for device security and privacy warnings and allow the visual communication of smart home configurations. We are interested in learning how smart home users experience interaction with those dashboards.

3 SYSTEM

SaferHome is an interactive system designed to help smart home users and bystanders keep track of their devices' locations and related security and privacy reports. Figure 2 provides an overview of SaferHome's architecture. Its *digital applications* are running on an Amazon Web Service (AWS) cloud tier. Household configurations, device reports, and usage data are stored on a DynamoDB database. The ReactJS application tracks the state of each household within the usage period and provides access according to the current study phase.

The *physical dashboard* is based on 16 custom-built printed circuit boards (PCBs), each featuring 16 connectors on a 10×10cm (3.9×3.9 inches) board. The PCBs, or tiles, are aligned in a 4×4 matrix, providing a configuration space of 40×40cm (15.7×15.7 inches) and 256 connectors. Within each tile, the location across the tile and its 16 connectors is determined based on a horizontal and vertical matrix of voltage dividers. The same concept applies to determining the location of a tile within the 4×4 matrix, as tiles are electrically connected in a series connection, with a single resistor acting as a voltage divider between two tiles. Smart home device proxies are made up of Arduino Nano microcontrollers and a 2×4 pin interface that connects to the 256 connectors. Once plugged in, the Arduino is powered by two of those pins. It determines its location on the board through an Analogue-to-Digital (ADC) conversion of three pins: the horizontal and vertical lines within the tile and the unique tile voltage itself. The device announces itself, its location, and its type (e.g., Voice Assistant, Alexa Echo Dot 2) with a unique ID to a Raspberry Pi 4 master through an I^2C interface integrated into the 256 connectors. Each proxy also features one yellow LED that can be turned on to attract attention to the specific device and to signal warnings. The physical dashboard's Raspberry Pi 4 master is connected to the internet and synchronizes the board's state with the SaferHome digital counterpart. To do so, the Pi 4 interfaces with cloud data storage. **This means that when users plug/unplug a proxy or move that proxy to a new location, SaferHome adjusts the digital dashboard accordingly. This allows us to easily track and sync changes made to the location and/or status of smart devices.**

3.1 Security and Privacy Reports

SaferHome provides information about the security and privacy vulnerabilities of the users' smart home appliances. As suggested by prior work [34], we convey the severity of a vulnerability using a traffic light metaphor. A green light means that no reports or only reports older than one year

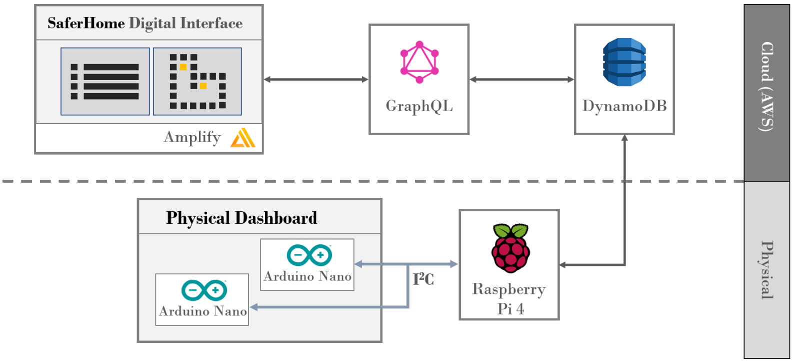


Fig. 2. Overview of SaferHome's architecture. The digital interfaces and data storage were running on an Amazon Web Service (AWS) cloud tier. The physical dashboard uses Arduino Nano microcontrollers as smart home proxies that interface with a Raspberry Pi 4 through an I^{2}C interface. The Raspberry mobile computer synchronizes changes directly with SaferHome's cloud data storage.

are available. A yellow light indicates that reports are available that are less than one year old. We refrained from using red lights since we manually assessed each device's privacy and security state. Thus, we could not guarantee to provide a decisive and complete picture which we clearly stated during the recruitment process and the consent form. We created these reports by searching publicly available databases[1] and conferring with a computer security consultant. As prior work suggested that merely informing users about privacy violations leads to frustration and privacy resignation [11, 36], we also give concrete recommendations on how to fix these vulnerabilities. An example of such a report is the following:

2019: Amazon Fire OS before 5.3.6.4 allows a man-in-the-middle attack against HTTP requests for "Terms of Use" and Privacy pages. **What can I do to fix these gaps?** Check if the device has the latest software installed, if not, perform an update.

3.2 Device Representations

Figure 1 depicts SaferHome's three device representations consisting of a *list view* and a *digital* and *physical dashboard.*

Digital List View: The list view (Figure 1a) as used by prior work [23, 34, 45] serves as the baseline condition and features a device list containing information about device types, manufacturers, models, and potential security and privacy vulnerabilities. Users can review the vulnerability reports at any time by clicking on the cells.

Digital Dashboard: In response to the call of previous work to provide users with a sense of the smart devices' locations [10, 45], we created a digital dashboard (see Figure 1b) that models the users' floor plans. For that, it features 256 configuration spots in a 16×16 matrix. In addition, it displays vulnerability reports when users hover over a device.

Physical Dashboard: The physical dashboard (see Figure 1c) is the counterpart of the digital dashboard. It features a surface area of 40×40cm (15.7×15.7 inches) and 256 connectors, where users can place wall tiles and functional device proxies. A proxy communicates the type of device through exchangeable icon plates placed on their top surface. Each proxy includes a bright yellow LED that turns on when vulnerability reports are available. The board is connected to the internet and synchronizes the state and location of connected device proxies. Household users can place

[1] https://cve.mitre.org/; https://nvd.nist.gov/products/cpe/search

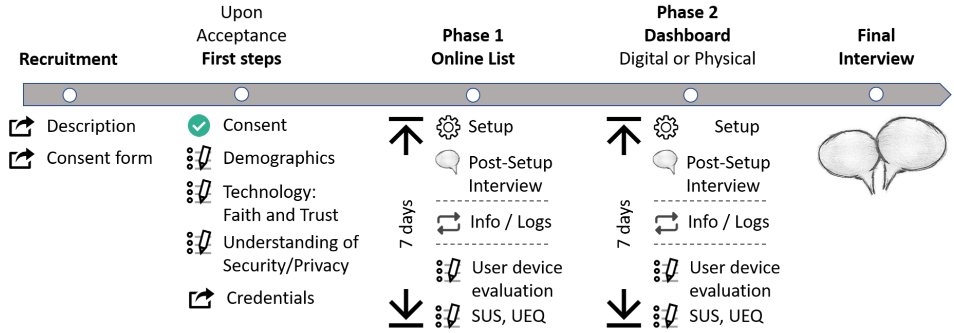


Fig. 3. Overview of the user study. Households experienced SaferHome's digital list for one week before switching to a floor plan dashboard for a second week. In the second week, households experienced either the physical and digital dashboards or only the digital ones. After using SaferHome for two weeks, we interviewed participating households briefly.

the board anywhere in their homes. We proposed study participants place the dashboard in the entrance hall to increase visibility.

4 METHOD

We conducted a mixed-method study with 16 participants from eight households. Each household member had access to SaferHome for two weeks, as shown in Figure 3. In the first week, participants reviewed their household devices and corresponding vulnerability reports through an online *list view* (see Figure 1a). In the second week, the household members had access to the digital and/or physical *dashboard*, representing actual floor plans and device locations (see Figure 1b-c). We studied how the use of SaferHome impacted smart home users' perceptions through a final interview.

4.1 Participants

We published a study description within our academic and social circles, i.e., university channels and social media, and asked interested parties for referrals to other smart home users. We shared an extended description and the consent form with interested parties during the recruitment process.

As shown in Table 1, we recruited eight households with two household members each, summing up to 16 participants. On average, households had 5.6 smart home devices (SD = 3.3). Households were assigned either to the digital or physical dashboard condition. The average age of all participants was 35 years (SD = 11.1 years). We recruited eight male and eight female participants. Table 1 further details participants' background and their technical affinity according to the 9-item Affinity for Technology Interaction (ATI) scale [17]. Finally, Table 1 also indicates device ownership. Inspired by [24], we asked every participant to self-assess for every connected device in their home to what degree they considered themselves as *pilots*, i.e., a person responsible for that device, or *passenger*, i.e., a person not responsible for purchasing and configuring that device. The information in Table 1 is based on an aggregated score across all devices and a linear scale involving five categories: pilot, mostly pilot, neutral, mostly passenger, and passenger.

4.2 Protocol

After all household members signaled acceptance to participate in the study, we asked each participant to complete a short survey, including questions about demographics (e.g., age, professional

Table 1. Overview of the participants and households. The table contains the household ID (HID), which dashboard variant they had (V., P = Physical, D = Digital), their number of smart devices (#), participant ID (PID), professional background, age, gender, technical affinity, and device ownership. Eight households (H1 - H8) participated with two household members each, meaning that 16 participants (P1 - P16) took part in the study.

HID	V.	#	PID	Background	Age	Gender	Technical Affinity	Device Ownership
H1	P	6	P1	Software developer	28	M	6.0 (Very High)	7.0 (Pilot)
			P2	Student (Art)	27	F	2.2 (Low)	3.2 (Mostly Passenger)
H2	D	5	P3	Videographer	29	M	5.2 (Very High)	7.0 (Pilot)
			P4	Student	26	F	3.0 (Medium)	3.4 (Mostly Passenger)
H3	P	4	P5	Recruiter	29	F	3.4 (Medium)	4.6 (Neutral)
			P6	Sales assistant	31	M	4.5 (High)	2.0 (Passenger)
H4	D	3	P7	Computer Scientist	25	F	4.5 (High)	2.7 (Mostly Passenger)
			P8	Radio Host	40	M	4.5 (High)	7.0 (Pilot)
H5	P	10	P9	Software developer	31	M	5.0 (Very High)	6.6 (Pilot)
			P10	L&D Specialist	28	F	3.3 (Medium)	2.9 (Mostly Passenger)
H6	D	11	P11	Managing Director	55	M	5.5 (Very High)	7.0 (Pilot)
			P12	Consultant	47	F	2.2 (Low)	2.5 (Mostly Passenger)
H7	P	5	P13	Mechanic	31	M	4.7 (High)	6.2 (Pilot)
			P14	Student (Medicine)	25	F	3.7 (Medium)	3.4 (Mostly Passenger)
H8	D	1	P15	Bank clerk	49	F	3.2 (Medium)	4.0 (Neutral)
			P16	Shop Assistant	58	M	3.8 (Medium)	6.0 (Pilot)

background), smart home ownership (pilot/passenger) [24], technical affinity [17], the tool functionality and helpfulness subscales adapted from the faith and trust in technology questionnaire by Mcknight et al. [32], and individual understanding of cyber security and privacy.

Phase I: Online List. We shared access credentials to SaferHome once each household member completed the initial survey. At this point, we organized a call to set up the device list on SaferHome, where users specified their devices' types, manufacturers, and models. The participants were supposed to enter all network devices except mobile phones, routers, laptops, and desktop computers. After they had specified all devices, we asked them about this configuration process and took notes. Initially, we displayed a message indicating that the device assessment process had started. However, we informed them beforehand that this was a manual process that could take 24 hours. Whenever the device analysis led to a vulnerability report, we published this report on SaferHome and notified each participant by email.

At the end of this first phase, we asked each participant to rate their devices. We used the statements of Oser et al. [34] inquiring about device risk concerns, monitoring, and removal acceptance. We also asked the users to complete the System Usability Scale (SUS) [9] and User Experience Questionnaire (UEQ) [26].

Phase II: Dashboard. The second week also started with a setup process observed by us. Households who used only the *digital* dashboard were asked to enter their floor plan and device locations on SaferHome. Devices stored in the previous round were pre-populated to ease the configuration. One of the authors visited households that got access to the *physical* dashboard. Here, the household members configured the physical dashboard by placing wall tiles and functional smart home device proxies. The proxies were prepared and programmed by us. Once the dashboard was fully configured, the observer asked about the setup experience. The physical user-configured floor plan setup was synced with the SaferHome cloud services, and the digital counterpart was created automatically.

Already existing assessments were synced to the digital and physical dashboards. We continued searching for device information and updates and informed users by email about changes. To complete the second phase, we repeated the survey about device selection, SUS, and UEQ.

Final Interview. After completing both phases, we invited households for a final semi-structured interview. Both household members were present at the interview. Initially, we asked about the experience of the past weeks in a very open manner to see if participants had already formed opinions they wanted to share. Next, we asked specifically about the difference in device representation, comparing the list to the floor plan dashboards and the digital to the physical dashboard. Finally, we asked participants to share suggestions for improvement.

5 QUALITATIVE RESULTS

We fully transcribed all interviews non-verbatim and analyzed them with Atlas.ti employing Thematic Analysis [8]. After familiarizing ourselves with the data, two authors conducted open coding of two interview transcripts. We extensively discussed the codes, merged and renamed them, and started constructing initial code groups. Next, one author coded the remaining interviews. Those codes were again discussed and assigned to the code groups. In total, we created 63 codes. We further discussed the resulting code groups in a third iteration and made minor adjustments. Ten code groups resulted from this iterative and collaborative process.

Out of those, we constructed three high-level themes: Awareness, Presentation, and Interaction. Related to **Awareness**, we reflect on smart home users' reported device privacy and security awareness and observed changes. We further show how study participants perceived the information value of the various views and elements in the context of the theme **Presentation**. Finally, in **Interaction**, we describe how users transformed information into privacy practices and reflect on SaferHome interaction in multi-user environments.

5.1 Awareness

In the context of this theme, our informants discussed (1) a change in privacy awareness resulting from SaferHome usage; (2) integration, or failure to do so, of privacy awareness into device purchase decisions; and (3) strategies to integrate SaferHome into users' smart home interaction.

Most of our study participants initially indicated that they were generally aware of *discussions and reports* around smart device privacy but had little interest or no means to take concrete actions related to their devices. Only members from one household, H3_P5, and H3_P6, explicitly reported researching device characteristics and reports before buying connected devices. Instead, our post-study interviews revealed that the SaferHome interaction increased several participants' privacy awareness and concern to the degree that they wished for further information and took concrete actions. For example, H7_P13 explicitly stated that SaferHome changed his view on connected devices: *"What has changed is that I check more often which software version I have, and whenever the lights lit up, I checked not only the devices that were directly affected but also whether the firmware of* *other devices was up to date."* In this context, H2_P3 and H2_P4 agreed that SaferHome pushed them towards reflecting on the security and privacy of their devices. P4 mentioned their dog camera as an example that tracked activities in the room, recorded videos on a cloud service, and allowed them to interact with their environment physically. H4_P7 further reported a form of *serendipitous* interaction with SaferHome based on her experience with the tool: *"I would also want to use it in the future to check from time to time whether there is something new for our devices and then act accordingly."*

Few participants further stressed that they did not know exactly what devices they had installed in their homes. For example, H7_P14, a user self-identified as *mostly passenger*, stated that she would like future systems to provide basic information on device types. She discussed network-attached storage (NAS) as an example device she would now like to know more about. Notably, one participant, H1_P2, *mostly passenger* as well, even indicated using some of the smart devices more frequently after using SaferHome: *"I use the devices more as I'm now more involved with them. Before the study, I wasn't so sure of what you could actually do with them."* These examples demonstrate how SaferHome supported some users in building a basic understanding of their smart home infrastructure and device capabilities.

Several informants reported considering new metrics for purchasing smart devices. In particular, H7_P13, H7_P14, and H8_P18 stressed that they would want to consider the manufacturer's size and country of origin. Notably, H1_P1 explained that device information would still be irrelevant to his purchase decisions. Rather, he would like SaferHome to track vulnerabilities and behaviors of connected devices while they are being used in their home: *"I don't think the dashboard would have such a strong influence when buying new devices but rather on the usage. In drastic cases, you can simply deactivate it again."* This view assumes that device issues, pre-existing or not, can and will likely be resolved, necessitating a tool that immediately informs about vulnerabilities and allows action.

Our informants reported several privacy concerns in response to the SaferHome interaction. Most discussed concerns regarding data collection and recording of voice assistants (H7_P13, H7_P14, H8_P15, and H8_P16). H7_P14, for example, stated: *"Whenever I interact with Alexa, I am now skeptical about it, and I am more aware that somehow data is collected no matter what you do"*. Additional concerns included fear of data breaches around network storage (H7_P14) and targeted marketing based on household conversations (H7_P13). Finally, we found that SaferHome users employed different strategies to integrate SaferHome into their smart home interaction. For example, H1_P1 and H1_P2 reported frequently reviewing the physical dashboard in order to remain updated about device information. In addition, most users reported that they started exploring device concerns and capabilities when they received email notifications. In this context, H3_P6 stressed that the LEDs attached to proxies on the physical dashboard created more awareness: *"The lights in the analog version are more noticeable. They confront you more than an email does."*

5.2 Presentation

This theme covers a range of experiences, interpretations, and requests around the presentation of information on digital and physical dashboards. In this context, almost all users stated that all dashboards they experienced were suitable to capture their household configurations. One household, H4, reported needing more fields on their digital floor plan dashboard to map their entire flat correctly. Another household, H8, indicated they needed a physical dashboard to map multi-level apartments.

The study participants extensively discussed the color coding of devices and associated threats. For example, H3_P6 wished for additional colors on the physical dashboard. The participant further stated that he would prefer a physical list-based dashboard with tangible device proxies and traffic lights over a physical floor plan dashboard limited to a single yellow warning light, arguing that *"I know where devices are located in the apartment, I don't necessarily have to review this on the dashboard."* H4_P7 also discussed a color coding experience with their digital dashboard. She described that they discussed their household when they observed that all smart lights turned yellow while all other devices remained green. Initially, they interpreted this as a visualization indicating that those devices were smart lights. They realized later that this visualization occurred by chance and that the yellow lights referred to medium-level warnings. The participant further discussed coloring the entire field according to the system's assessment to prevent misinterpretation.

H2_P3 proposed developing an additional and more traditional dashboard that would be better suited for a larger number of smart home devices: *"Imagine a bigger household with 40 devices. To get a quick overview. An index that represents overall safety. [...] It could be an overview that indicates that 30 out of 40 devices work as expected and that security issues were detected for five devices [...]"*. Here, the interviewee imagined an even simpler, more general metric for the entire household, represented by a single index. Such a dashboard, or an evolution of the current ones, could support additional user requests. For example, H7_P13 asked for more information about the kinds of data transmitted by smart home devices: *"I would like to find out how much and what data is sent overall. Is it only a couple of encrypted megabytes or exact information like my birthday?"* This is closely related to the request from H7_P14, who wanted to know in more detail how devices behaved, particularly how much voice assistants recorded and transmitted.

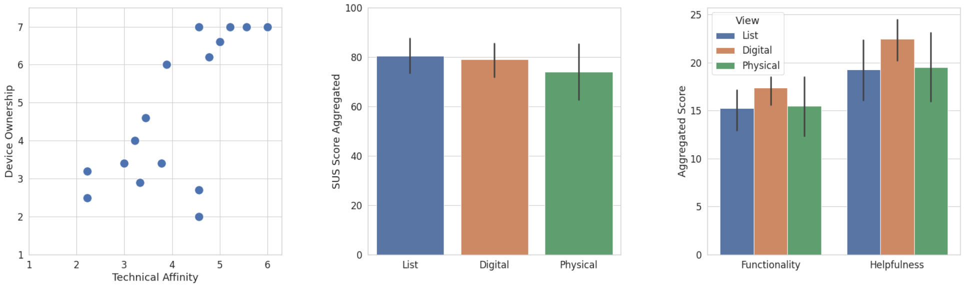
Overall, the study participants expressed that the interpretations of device threats, recorded in the digital views of SaferHome and in the email notifications, were helpful. Yet, H1_P1 and H7_P14 asked for more concrete instructions on how to handle issues. In this context, also H7_P13 stressed that he expected the tool to play a more active role in resolving reported issues. He explained that once, after clicking on *'Okay'* on a device warning page, he was unsure whether this had actually resolved the described issue: *"When I clicked okay, I was unsure whether that had fixed the issue. Initially, I expected the light to change to green or go out."* This example shows that SaferHome profits from a clearer description of its limitations concerning issue handling.

5.3 Interaction

Based on the previous themes, we understand that the interaction experience is partly shaped by the threat presentation and SaferHome's interpretation of device information. This experience impact users' privacy concerns and awareness evolution. Within the theme INTERACTION, we collected additional experiences and requests related to personalization, multi-user interaction, and advanced features.

Smart homes, their users, and the relationships between household members are unique. This understanding is also represented in our data. Several participants stressed that they wished to receive updates only for devices they considered critical to their privacy. H3_P5 further wished for a feature that would allow her to manually reset a warning light after checking the associated reports: *"That I can say: Okay, I have checked it. The lamps should now be green again."* These are desired control features that relate to forms of framework personalization. H1_P1 discussed an additional aspect: personalization of proposed solutions. The interviewee stressed that the system would need to distinguish between expert users and normal users: *"It would be simple, of course, to log in to your router and block the port, which, however, would likely overwhelm 95% of all people. And for the other 5%, this would not be sufficient, as it does not really solve a problem."*

Our data analysis confirmed that users with lower technical affinity and device ownership expressed not knowing about device capabilities more often. The following statement made by H7_P14 echoed this and further reveals that passenger users might not know about all installed devices: *"(P13) bought everything and knows better what is installed."* Regarding concrete actions,



(a) (b) (c)

Fig. 4. **(a)** Overview of key characteristics related to users' technical affinity and sense of device ownership. **(b)** Overview of user ratings concerning the System *Usability* Scale (SUS) [9] and **(c)** tool *functionality* and *helpfulness* of SaferHome's views.

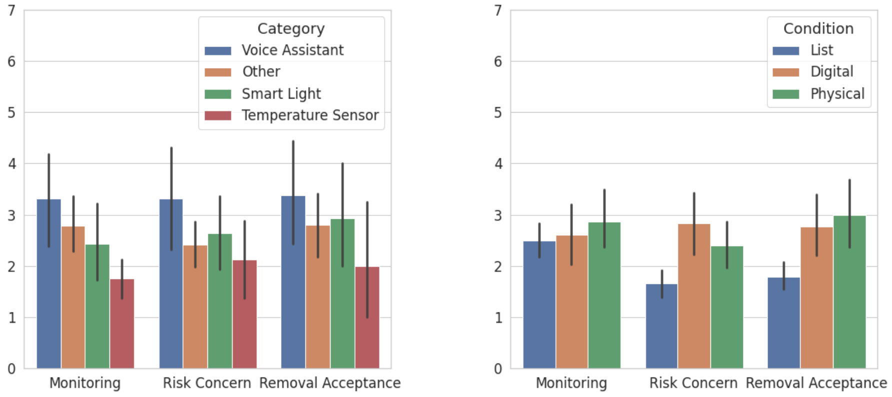
both pilot and passenger household members described their high expectations of firmware updates. Asked about SaferHome's impact on future purchase behavior, both H4_P7 (mostly passenger) and H4_P8 (pilot) echoed not adapting their device selection criteria. Rather, they want to rely on manufacturers to update any existing or future vulnerabilities. Participants further expressed creating awareness of the importance of smart device firmware updates. H7_P13 reported checking the digital dashboard explicitly to compare current firmware versions with versions reported in security warnings. H4_P7 described immediately updating a smart light bridge after she reviewed SaferHome's threat analysis. Finally, H3_P5 stressed that she finds it difficult to check which firmware versions are currently installed on the smart devices and whether or not automatic updates have been performed. Both household members stated that they would want SaferHome to research and display current firmware versions: *"I would like the dashboard to compare the software versions itself and then, if the correct software is not installed, initiates the update" (H3_P6).*

Those requests are part of the advanced features described and desired by our participants. Additional features were related to the network itself. H2_P3 imagined that the system could be extended to cover network components further. H1_P1 stressed that the physical dashboard could support advanced network features. The participant referred to PiHole as a technology and application that could help to filter directly and block traffic of selected devices, thereby creating a link between dashboard device proxies and their real capabilities and actions.

6 QUANTITATIVE RESULTS

We conducted an exploratory quantitative analysis of the participants' (1) technical affinity and device ownership, (2) perceived qualities of SaferHome and (3) perceptions of smart devices. We conducted all analyses with Scipy v1.6.3 and statsmodel v0.12.2. All bar plots in this section display error bars that show the 95% confidence interval. Given our sample size, the quantitative analysis mainly supplements our qualitative findings.

Participants' Technical Affinity and Device Ownership. As shown in Table 1, there was no household with only *pilots* (i.e., pilot or mostly pilot) or only *passengers* (i.e., passenger or mostly passenger). Figure 4a depicts the distribution of technical affinity and device ownership. We ran a Spearman's correlation to determine the relationship between technical affinity and device



(a) (b)

Fig. 5. Monitoring, risk concern, and removal acceptance according to **(a)** device category and **(b)** SaferHome view. Both plots are based on ratings recorded after the second phase ended.

ownership, which revealed a strong positive monotonic correlation between technical affinity and device ownership ($r_s = .69$, $n = 16$, $p < .05$).

SaferHome's Usability, User Experience, Functionality, and Helpfulness. There were no significant differences between SaferHome's three views related to their usability (see Figure 4b), user experience, and tool functionality and helpfulness (see Figure 4c). Yet, we note that the usability and user experience ratings of all three views are consistently within the range or above established average values[2,3].

Monitoring, Risk Concern, and Removal Acceptance of Smart Devices. As depicted in Figure 5a, we find that our participants expressed a higher risk concern, removal acceptance, and willingness to monitor devices of the category *voice assistant*, as compared to devices of other categories. In contrast, Figure 5b provides an overview of monitoring, risk concern, and removal acceptance in the context of the dashboard that was used. We find that participants expressed a significantly ($p < 0.05$) higher risk concern and removal acceptance for the devices after using the floor plan dashboards, as compared to the digital list view in phase one.

7 DISCUSSION

We presented SaferHome, a digital-physical smart home privacy framework. In contrast to SAFER [34], which was limited to mock data, mock devices, a brief interaction, and a digital list view, we developed a functional framework with three views, including an interactive physical one, that is designed to manage real household configurations. In line with Wash and Rader [41], who stressed that mapping users' device security decisions require understanding their context, we evaluated SaferHome with eight households in a two-week study. In this section, we first discuss our findings through the lenses of our two research questions and present implications for the design of future

[2] SUS scores above 70 are often interpreted as *acceptable*, *"with better products scoring in the high 70s to upper 80s"* [4]

[3] UEQ benchmarks show that SaferHome views were, with the exception of physical dashboard stimulation, consistently rated above average, good, or excellent. [39]

smart home privacy frameworks. Second, we present challenges to developing ubiquitous smart home privacy dashboards.

RQ1: How does SaferHome impact privacy awareness of smart home users? We asked our study participants about their privacy concerns and privacy practices before and after using SaferHome for two weeks. Our findings are consistent with literature showing that users currently do not strongly consider privacy factors when choosing new devices [13, 34]. While most smart home users in our study had heard about smart device privacy issues, they did not evaluate threats to their own privacy as serious or reported not having had access to tools that would support them in making decisions. This is in line with findings from previous work that found the privacy policies of smart speakers insufficient in informing users about how their data is handled [1]. Yet, this perception partly changed across most participants after using SaferHome for two weeks as they reflected more on their installed devices, capabilities, and potential exposures. This was particularly true for voice assistants. Several participants further reported checking the firmware versions of their devices and searching for updates. In multiple cases, this process even included devices not evaluated as *devices of concern*. In this context, several households reported worrying less about privacy threats and device purchases post-study, as tools like SaferHome would help keep devices updated. This echoes findings from previous work that uncovered a need to provide users with adequate tools as they often did not know how to limit or control the data collected by smart speakers [1]. As such, tools like SaferHome can be powerful measures to hand users back control over their data as they give concrete hints on fixing security issues. However, we argue that while providing users with device warnings and interpretations focused on concrete firmware versions and updates certainly helped to secure smart home networks, future privacy framework designers **need to communicate that privacy threats are not limited to known and displayed security vulnerabilities**. Rather, they must create user awareness of additional threats, including unknown vulnerabilities and privacy violations, by design. In this context, an interesting metric to further explore could be manufacturers' *past update behavior*, as Oser et al. [34] imagined in their conceptual showcase. This could indicate device manufacturers' responsiveness and be a helpful metric for device selection.

Our work provides insight into device ownership and responsibility across real smart home configurations and setups. We found a clear separation between passenger and pilot users [24] across all households. Several interviews demonstrated that the *passenger* user had less knowledge about devices installed in their homes. None of those participants stressed that they were particularly concerned about learning about the devices, their capabilities, and potential threats through the study. Still, several users indicated that they wanted to take this opportunity to learn more about the different types of smart devices and called for basic information to be integrated into SaferHome. We argue that, in particular, the physical dashboard, as well as the joint configuration across all SaferHome views (see Figure 1a-c) helped create interest and awareness across all household members, including passenger ones. Thus, we suggest that future systems should design interactive experiences that **require all household members to join the configuration and review process to avoid the imbalance between passenger and pilot users further extends into decisions around device privacy monitoring**.

RQ2: How do smart home users experience the interaction with dashboards that map floor plans? Our results show that the study participants perceived the three SaferHome views, i.e., digital list view, digital dashboard, and physical dashboard (see Figure 1a-c), similar across usability, user experience, tool functionality, and tool helpfulness. This is notable considering that the physical dashboard provided less information directly to the smart home users. Still, they rated the physical dashboard similar to the digital views that directly displayed device warnings. We argue that this can partly be explained by the added value described by our study participants: the constant exposure to their smart home configuration that led to frequent reflections about installed devices and their locations. In this context, one participant even stated that the single-color LED attached to physical dashboard proxies created more awareness and urgency to act than the detailed information received via email. Still, we argue that there is a need to **further explore design that balances between SaferHome's easy-to-use physical device proxies and users' need for additional information and control.**

This call for control was further echoed by several participants asking for advanced interactive features. Two participants described that the physical dashboard should directly interface with network devices and possibly filter or sanction their remote data exchange. That way, users manipulating the physical dashboard could adjust the smart home configuration directly to their current contextual privacy preferences. In combination with device proxy features that represent and communicate device states, this could turn dashboards into powerful privacy tools. We argue that the tangibility and ease of access to the physical dashboard played a strong role in developing this user vision for advanced interactive features. Still, we emphasize that additional control features will also benefit digital dashboards. We suggest that future system designers **explore dashboards and their device proxies, digital and physical, as interactive spaces that allow to adjust and monitor device privacy settings directly.**

Finally, we note that one interviewee asked for a physical list-based dashboard that would allow tracking a larger number of smart home devices. The participant argued that this was more useful as he already knew the location of devices installed in the household. While this might be true in this specific case, other participants echoed that the constant reminder of where devices were physically placed was useful. In this context, we note that none of the participants explicitly referred to the dashboards as device privacy communication channels for their interaction with visitors. Only one household, H3, reported having had a visitor over during their study participation. In this case, the mother of H3_P5 noted the physical dashboard and inquired about it. The household members reported that she was curious but did not use the dashboard to engage in further discussions or negotiations. We note that future researchers could **explore over an extended period of time how floor plan dashboards, physical and digital, impact actual smart home privacy negotiations between owners and bystanders**. Our dashboards might represent a basis for such explorations that would extend literature [30, 44] with lived experiences.

7.1 Towards Ubiquitous Smart Home Privacy Dashboards

Finally, we present additional research and design challenges for future smart home privacy frameworks and dashboards informed by our findings and related work.

Visibility and Trust. Our findings indicate that dashboard visibility and recall impact the device privacy awareness of smart home users. This was especially true for the participants experiencing the physical dashboard. Future system designers might explore dedicated smart home screens as an accessible medium to display device privacy dashboards. However, we note that screen-based solutions risk smart home users switching privacy information for more entertaining ones (e.g., videos or chat notifications). As such, we suggest to **further explore physical and tangible solutions as smart home privacy dashboards**.

We found that a few users did not find the floor plan particularly useful, as they indicated knowing what kind of devices they had installed. Yet, research has shown that bystanders, i.e., guests and family members, find it difficult to know about and assess smart devices [30, 44]. Here, physical privacy dashboards that cannot be transformed for another purpose could help communicate the existence and context of smart devices reliably. This might even address issues in more public spaces like hotels and vacation rentals [29]. Yet, research into this space should **explore how to certify**

information represented on the dashboards, as there is a risk that erroneous configurations and manipulated dashboards could be misused to provide a false sense of security to smart home bystanders.

Device Landscape. Several participants requested to assess additional devices, including mobile phones and network components. Researching how to integrate low-level infrastructure hardware and non-stationary devices across different dashboard views is an important challenge.

Personalization. Our findings are in line with those of Wash and Rader [41] who argued that *"educating users about security is not simply a more-is-better issue, and not all users should receive the same messages."* Rather, we find that basic device information and threat interpretations should be tailored to users' technical affinity and device ownership. Yet, we also need to develop an understanding of **how to personalize assessments without reducing the information value for selected users**. Doing so would further risk increasing the imbalance between different user types.

7.2 Limitations and Future Work

To enable future research, we share the development Github repository[4] that contains the source code for the cloud and hardware applications.

We recognize that a diverse sample is key in studying smart device privacy concerns and privacy practices. To this end, we recruited participants with diverse professional backgrounds. Our sample, half female, and half male, covers participants between 25 and 58 years old. Yet, we also note as a limitation that we only recruited participants living in Germany. Thus, users' privacy practices, technical affinity, device ownership, and interpersonal communication habits might be biased by a Western European mindset. In addition, we note that all participating households had two members, one male and one female. Thus, research should consider sampling across additional cultural backgrounds, single-user households, and larger households. In this context, we also note that future research across larger user populations should focus more on collecting quantitative user data. Our sample of 16 participants across eight households allowed us to create in-depth qualitative insights. Yet, we explicitly note the explorative and purely complementary character of the quantitative data analysis as a limitation.

We chose to start the two-weeks study phase always with the baseline condition, i.e., the digital list view. We decided against counterbalancing the conditions to slowly introduce users to new interface elements. As the security reports already represented new elements users had to learn to incorporate into their routines, we introduced them together with the conventional list view. We combined them with the new representation as floor plans only after one week. This way, we hoped not to overwhelm the users and make the process more understandable. However, we acknowledge that this might have introduced effects on users' perception and, thus, ratings of the different representations. Hence, future work should investigate how to find the best trade-off between order effects and introducing users to new dashboard representations.

The dashboards show the devices in a home with their associated vulnerability reports subdivided into four overarching groups (voice assistants, smart lights, temperature sensors, and others). These groups are insufficient to cover all the different types of sensors smart home devices employ or devices that combine multiple sensors, such as smart displays that have microphones and cameras. Yet, we know from previous work that devices evoke very different privacy concerns depending on the sensors they leverage. While microphones and cameras evoke the biggest privacy concerns, temperature and motion sensors are generally not perceived as very concerning [42]. As such, a fine granularity in displaying the types of sensors is important to accommodate users' varying

[4] https://github.com/mimuc/SaferHome

privacy concerns. Consequently, future research should investigate how information about the classes of sensors can be integrated into smart home dashboards.

8 CONCLUSION

We reported on the design and empirical evaluation of SaferHome, a digital-physical privacy framework for smart home users. In contrast to related work focused on qualitative studies and concept showcases, we evaluated SaferHome with eight households and 16 participants in the wild. In a two-week study, all participants mapped their actual smart home configurations on multiple dashboards. In the first week, all households used a digital list view. In the second week, they used physical or digital dashboards that allowed them to map floor plans and device locations of their smart home setups. The users received real device privacy and security analyses across all three dashboards. Our evaluation showed that smart home users were particularly concerned about voice assistants. Further, we found that the constant recall provoked by the physical dashboard led to an increased reflection. Generally, the participants stressed that the dashboards based on floor plans helped to consider the devices' context of use. Based on our findings, we presented design implications and research challenges that consider users' technical affinity and sense of device ownership. We hope our findings will help design future smart home privacy frameworks that allow individuals and communities to make informed and transparent decisions.

REFERENCES

[1] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 451–466. https://www.usenix.org/conference/soups2019/presentation/abdi

[2] Abdulaziz Abdugani. 2020. Privacy Analysis of Smart TV Communication: A case study of privacy threats in Smart TVs. (2020).

[3] Maggie Astor. 2017. Your Roomba may be mapping your home, collecting data that could be shared. *The New York Times* 25 (2017).

[4] Aaron Bangor, Philip T Kortum, and James T Miller. 2008. An empirical evaluation of the system usability scale. *Intl. Journal of Human–Computer Interaction* 24, 6 (2008), 574–594.

[5] The BBC. 2019. *Smart speaker recordings reviewed by humans.* https://www.bbc.com/news/technology-47893082

[6] France Bélanger and Robert E Crossler. 2011. Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly* (2011), 1017–1041.

[7] Giampaolo Bella and Lizzie Coles-Kemp. 2012. Layered analysis of security ceremonies. In *IFIP International Information Security Conference*. Springer, 273–286.

[8] Ann Blandford, Dominic Furniss, and Stephann Makri. 2016. *Qualitative HCI Research: Going Behind the Scenes.* Morgan & Claypool Publishers, 51–60. https://doi.org/10.2200/S00706ED1V01Y201602HCI034

[9] John Brooke et al. 1996. SUS-A quick and dirty usability scale. *Usability evaluation in industry* 189, 194 (1996), 4–7.

[10] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. *"It Did Not Give Me an Option to Decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products.* Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445691

[11] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. 2020. *Informing the Design of a Personalized Privacy Assistant for the Internet of Things.* Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376389

[12] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the experts: What should be on an IoT privacy and security label?. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 447–464.

[13] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300764

[14] ENISA. 2017. *ENISA Baseline Security Recommendations for IoT.* https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[15] ENISA. 2019. *ENISA IoT Security Standards Gap Analysis.* https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis

[16] Marcia Ford and William Palmer. 2019. Alexa, are you listening to me? An analysis of Alexa voice service network traffic. *Personal and Ubiquitous Computing* 23, 1 (2019), 67–79.

[17] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A personal resource for technology interaction: development and validation of the affinity for technology interaction (ATI) scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467.

[18] Ester Fritsch, Irina Shklovski, and Rachel Douglas-Jones. 2018. Calling for a Revolution: An Analysis of IoT Manifestos. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. ACM, New York, NY, USA, Article 302, 13 pages. https://doi.org/10.1145/3173574.3173876

[19] Gartner. 2019. *Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020.* https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io

[20] Christine Geeng and Franziska Roesner. 2019. *Who's In Control? Interactions In Multi-User Smart Homes.* Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300498

[21] Marco Ghiglieri and Erik Tews. 2014. A privacy protection system for hbbtv in smart tvs. In *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*. IEEE, 357–362.

[22] Richard Harper et al. 2011. *The connected home: The future of domestic life.* Springer.

[23] Xin Huang, Paul Craig, Hangyu Lin, and Zheng Yan. 2016. SecIoT: a security framework for the Internet of Things. *Security and communication networks* 9, 16 (2016), 3083–3094.

[24] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. 2021. *"We Just Use What They Give Us": Understanding Passenger User Perspectives in Smart Homes.* Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445598

[25] Hyosun Kwon, Joel E. Fischer, Martin Flintham, and James Colley. 2018. The Connected Shower: Studying Intimate Data in Everyday Life. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 4, Article 176 (dec 2018), 22 pages. https://doi.org/10.1145/3287054

[26] Bettina Laugwitz, Theo Held, and Martin Schrepp. 2008. Construction and evaluation of a user experience questionnaire. In *Symposium of the Austrian HCI and usability engineering group*. Springer, 63–76.

[27] Roxanne Leitão. 2019. In *Proceedings of the 2019 on Designing Interactive Systems Conference* (San Diego, CA, USA) *(DIS '19)*. Association for Computing Machinery, New York, NY, USA, 527–539. https://doi.org/10.1145/3322276.3322366

[28] Franco Loi, Arunan Sivanathan, Hassan Habibi Gharakheili, Adam Radford, and Vijay Sivaraman. 2017. Systematically Evaluating Security and Privacy for Consumer IoT Devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy* (Dallas, Texas, USA) *(IoTS&P '17)*. ACM, New York, NY, USA, 1–6. https://doi.org/10.1145/3139937.3139938

[29] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (2020), 436–458. https://doi.org/10.2478/popets-2020-0035

[30] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You Just Can't Know about Everything": Privacy Perceptions of Smart Home Visitors. In *19th International Conference on Mobile and Ubiquitous Multimedia* (Essen, Germany) *(MUM 2020)*. Association for Computing Machinery, New York, NY, USA, 83–95. https://doi.org/10.1145/3428361.3428464

[31] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. 2020. "I Don't Know How to Protect Myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society* (Tallinn, Estonia) *(NordiCHI '20)*. Association for Computing Machinery, New York, NY, USA, Article 4, 11 pages. https://doi.org/10.1145/3419249.3420164

[32] D Harrison Mcknight, Michelle Carter, Jason Bennett Thatcher, and Paul F Clay. 2011. Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems (TMIS)* 2, 2 (2011), 12.

[33] David H. Nguyen, Alfred Kobsa, and Gillian R. Hayes. 2008. An Empirical Investigation of Concerns of Everyday Tracking and Recording Technologies. In *Proceedings of the 10th International Conference on Ubiquitous Computing* (Seoul, Korea) *(UbiComp '08)*. Association for Computing Machinery, New York, NY, USA, 182–191. https://doi.org/10.1145/1409635.1409661

[34] Pascal Oser, Sebastian Feger, Paweł W. Woundefinedniak, Jakob Karolus, Dayana Spagnuelo, Akash Gupta, Stefan Lüders, Albrecht Schmidt, and Frank Kargl. 2020. SAFER: Development and Evaluation of an IoT Device Risk Assessment Framework in a Multinational Organization. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 4, 3, Article 114 (Sept. 2020), 22 pages. https://doi.org/10.1145/3414173

[35] Pascal Oser, Frank Kargl, and Stefan Lüders. 2018. Identifying Devices of the Internet of Things Using Machine Learning on Clock Characteristics. In *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*. Springer, 417–427.

[36] Sameer Patil, Roberto Hoyle, Roman Schlegel, Apu Kapadia, and Adam J. Lee. 2015. Interrupt Now or Inform Later? Comparing Immediate and Delayed Privacy Feedback. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 1415–1418. https://doi.org/10.1145/2702123.2702165

[37] Edoardo Pignotti and Peter Edwards. 2013. Trusted Tiny Things: Making the Internet of Things More Transparent to Users. In *Proceedings of the International Workshop on Adaptive Security* (Zurich, Switzerland) *(ASPI '13)*. ACM, New York, NY, USA, Article 2, 4 pages. https://doi.org/10.1145/2523501.2523503

[38] Daniel Schatz, Rabih Bashroush, and Julie Wall. 2017. Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law* 12, 2 (2017), 8.

[39] Martin Schrepp, Andreas Hinderks, and Jörg Thomaschewski. 2017. Construction of a Benchmark for the User Experience Questionnaire (UEQ). *Int. J. Interact. Multim. Artif. Intell.* 4, 4 (2017), 40–44.

[40] Los Angeles Times. 2016. *Our privacy is losing out to Internet-connected household devices.* https://www.latimes.com/business/la-fi-lazarus-20160115-column.html

[41] Rick Wash and Emilee Rader. 2015. Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 309–325. https://www.usenix.org/conference/soups2015/proceedings/presentation/wash

[42] Maximiliane Windl and Sven Mayer. 2022. The Skewed Privacy Concerns of Bystanders in Smart Environments. *Proc. ACM Hum.-Comput. Interact.* 6, MHCI, Article 184 (sep 2022), 21 pages. https://doi.org/10.1145/3546719

[43] WIRED. 2019. *Don't Get Your Valentine an Internet-Connected Sex Toy.* https://www.wired.com/story/internet-connected-sex-toys-security/

[44] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 59 (Nov. 2019), 24 pages. https://doi.org/10.1145/3359161

[45] Eric Zeng and Franziska Roesner. 2019. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA, 159–176. https://www.usenix.org/conference/usenixsecurity19/presentation/zeng

Received 2022-07-05; accepted 2022-09-24