Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes

Maximiliane Windl
LMU Munich
Munich, Germany
Munich Center for Machine Learning
Munich, Germany
maximiliane.windl@ifi.lmu.de

Albrecht Schmidt
LMU Munich
Munich, Germany
albrecht.schmidt@lmu.de

Sebastian S. Feger
LMU Munich
Munich, Germany
sebastian.feger@ifi.lmu.de

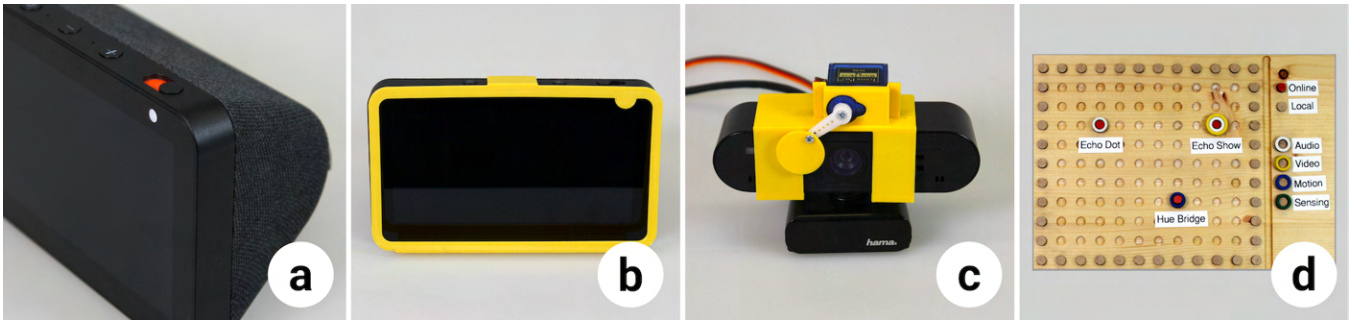

Figure 1: Overview of our tangible privacy artifacts. a) Shows the integrated tangible camera shutter of an Echo Show. b) Depicts our 3D printed Snap-on-Privacy (SNOP) artifact to cover the Echo Show's camera as used in studies I and II. c) Shows our automated 3D printed SNOP artifact on a webcam as used in studies I and II. d) Shows the tangible, static smart home dashboard from study III. It shows one room with three smart devices: an Echo Dot, an Echo Show, and a Hue Light Bridge. The rings depict the device sensors, and the colored pins depict whether a device is connected to the internet or the local network.

ABSTRACT

Most smart home devices have multiple sensors, such as cameras and microphones; however, most cannot be controlled individually. Tangible privacy mechanisms provide control over individual sensors and instill high certainty of privacy. Yet, it remains unclear how they can be used in future smart homes. We conducted three studies to understand how tangible privacy mechanisms scale across multiple devices and respond to user needs. First, we conducted a focus group (N=8) on speculative tangible control artifacts to understand the user perspective. Second, we ran a workshop at a human-computer interaction conference (N=8) on tangible privacy. Third, we conducted a six-week in-the-wild study with a tangible, static privacy dashboard across six households. Our findings help to contrast the need for tangible privacy mechanisms on the sensor level with user needs on a smart home level. Finally, we discuss our design implications for future smart homes through the lens of inclusive privacy.

CHI '23, April 23–28, 2023, Hamburg, Germany

ACM ISBN 978-1-4503-9421-5/23/04…$15.00
https://doi.org/10.1145/3544548.3581167

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; **Social aspects of security and privacy**.

KEYWORDS

Privacy, Configurable Smart Devices, Speculative Design, Inclusive Privacy, Tangible Privacy Spectrum.

ACM Reference Format:
Maximiliane Windl, Albrecht Schmidt, and Sebastian S. Feger. 2023. Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23), April 23–28, 2023, Hamburg, Germany*. ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3544548.3581167

1 INTRODUCTION

The number of smart devices in private spaces is constantly growing as they provide comfort by automating tedious tasks such as watering plants, controlling lights, adjusting temperatures, or cleaning. To complete these tasks successfully, the devices are equipped with sensors that constantly collect and process data. However, this becomes problematic when the data is abused for malicious intents and exploited to infer sensitive information, reveal identities, or track user behavior [2, 42, 47]. Yet, not only the owners and primary users of smart devices are exposed to these dangers but everyone in their vicinity. So-called bystanders, i.e., people who are not the primary users but are nevertheless exposed to technology, have been

recognized as especially protection-worthy as they often have limited control options to protect themselves [30, 31, 36, 37, 60]. Even though most people are unsure about the concrete dangers posed by smart devices [19, 34, 35], many still feel uncomfortable in their vicinity and can name concerns when explicitly asked [29, 30, 57]. This clearly shows the need to hand all stakeholders in smart homes adequate tools to regain autonomy over their privacy.

Prior work has shown that the sensor type strongly influences the level of concern; while microphones and cameras evoke the biggest concerns, temperature and motion sensors are perceived as less concerning [9, 45, 57]. As many smart devices bundle multiple sensor types in one device, granular control on the sensor level is needed to accommodate this divergent threat perception. However, currently, smart devices only have one common control option: turning the device off. While this solution is clearly unsatisfactory, it also fails to scale in increasingly complex and device-rich smart homes. Hence, we require supplementary interventions to achieve such granular control.

"Tangible Privacy" has been proposed as an effective means to control individual sensors as it provides "clear confidence and certainty of privacy to observers" [1]. Consequently, Ahmad et al. [1] call for each sensor in a smart home to have tangible mechanisms to allow control over data collection and give unambiguous feedback by clearly communicating what data is currently collected. Yet, existing prototypes enabling tangible control over individual sensors are mostly contained within the research domain [10, 14, 26, 53], and thus it is unclear whether they match the users' expectations and needs.

In response to the call for tangible privacy on a sensor level, we investigated physical privacy-preserving mechanisms for future smart homes across three studies and a rich mix of methods. In particular, we aimed to contrast the user experience around tangible privacy mechanisms with their control in increasingly complex smart homes. First, we developed speculative artifacts for granular tangible control, which we investigated in a focus group and co-design activities with eight participants. We found that tangible control artifacts are appreciated but should be bundled in a central control unit. Additionally, we uncovered tensions and possible conflicts around divergent privacy needs and desired comfort provided by smart devices. Second, to supplement the insights from the focus group with academic insights, we conducted a workshop at a human-computer interaction (HCI) conference on tangible privacy mechanisms (N=8). We found that the workshop participants focused on analog methods, such as punch cards, to store privacy profiles to prevent digital attacks. Moreover, they designed mechanisms to increase awareness instead of providing control. Third, aligned with the insights from the previous two studies, we prototyped and deployed a tangible, static privacy dashboard in a six-week in-the-wild study across six households to investigate how different stakeholders interact with it and gain insights into real-world privacy negotiations. We found that the dashboards increased awareness for owners and visitors. Moreover, it sparked numerous conversations about smart home privacy. Yet, while visitors frequently expressed discomfort, they seldom asked directly to switch devices off because they did not consider their data sensitive or avoided social conflict.

Our contribution is twofold: (1) we present findings from three studies that map needs and requirements around tangible privacy control through a rich set of methods, including participants with differing ages and backgrounds for studies I and III and participants with a background in HCI for study II; and (2) we discuss design implications for complex future smart homes through the lens of inclusive privacy.

2 RELATED WORK

In the following, we reflect on the role of privacy in smart homes and detail what peoples' specific concerns are. We then present work around the different roles of smart device owners and bystanders, including possible tensions. After that, we present current solutions for control in smart homes and show how our research around the control of tangible privacy-preserving mechanisms addresses some of their shortcomings.

2.1 Privacy in Smart Homes

As smart devices are placed in the most intimate spaces, they are capable of revealing exceptionally sensitive information when exploited. Obermaier and Hutle [47] and Apthorpe et al. [2] found that data collected by smart homes can be used to reveal identities and track user behavior. For instance, it was shown that data collected from smart meters could reveal the number of people in a household, their sleeping routines, and eating habits [42]. Additionally, Obermaier and Hutle [47] showed how video surveillance systems could be exploited to inject forged video streams or reveal possibly sensitive video data. *This clearly shows the need to protect users' privacy as smart devices can exploit most private information.*

While users are often unsure about the exact dangers and vulnerabilities of smart devices [19, 34, 35], many still have concerns when in their vicinity [57]. Such concerns include devices transmitting data without explicit consent [29] or, in regards to smart speakers, always listening, using this information for targeted advertising, and sharing it with third parties [30]. In relation to concrete data types, users are most concerned about demographics such as age or gender or communication and activity data [5]. Yet, researchers found that whether or not the misuse of data is perceived as sensitive depends on situational sense-making and is therefore subject to change [28]. When it comes to sensors, users are most concerned about microphones and cameras [9, 45], while temperature and motion sensors do not nearly raise the same level of discomfort [57]. Moreover, users are often even skeptical that smart devices without microphones and cameras cause any threats to their privacy [8, 11, 61]. *As prior research found that users are concerned about smart devices, we need to offer them control options to hand them back autonomy over their personal data. In addition, as different sensors raise different levels of concern, granular control is required to accommodate this divergent perception.*

Often, bystanders can not consciously decide to engage with a smart device but are implicitly forced to interact. Such cases can occur when visiting a friend that has a smart doorbell or staying at an Airbnb with a smart security system. In this work, we define bystanders as people who are not the owner or primary users of a smart device but are nevertheless exposed to it. This power imbalance caused by missing ownership and lacking technical affinity

becomes especially concerning when exploited in abusive partnerships [31]. Moreover, bystanders usually have no option to engage with smart devices' privacy regulations beforehand [30]. Yao et al. [60] explicitly investigated bystanders' privacy concerns in smart homes by confronting them with different scenarios. They found that they were most uncomfortable with devices that captured audio and video and in temporary resident and playdate scenarios. In addition, Marky et al. [37] found that smart home visitors are often unaware of being tracked and unable to protect their privacy effectively. In the context of Airbnb rentals, Mare et al. [36] found that guests were most concerned about getting discriminated against due to their behavior captured by smart devices, being spied on by the hosts, or experiencing security risks due to hosts not securing their smart devices. *Prior work shows that bystanders are especially protection worthy due to their inability to engage with privacy regulations or exert control over smart devices. Thus, we need to provide tools that allow them to make informed privacy decisions.*

2.2 Privacy Control

Providing users with control to limit and manage the collection of their personal data has long been seen as an effective means to protect their privacy. Earlier research focused on privacy on the web. Here, Reeder et al. [48], for example, proposed a new visualization in the form of an expandable grid for privacy policies to make them easier to understand and ultimately increase users' privacy control online. Later research on web privacy suggested, for example, visualizing privacy policies similar to nutrition labels [25] or displaying only short snippets in the users' context of use [55]. This visualization is in line with the principle of contextual integrity [46] that states that context is vital to decide whether data collection is appropriate. Following this principle, Jia et al. [23] developed a context-based permission system for IoT environments to help users effectively control access to their personal data. Recent research has also focused on tools for privacy control outside of the web, for example, on smartphones through privacy dashboards [6, 18], or in the IoT through a personalized privacy assistant that is envisioned to make automatic privacy-relevant decisions on the users' behalf [12]. Here, Feng et al. [16] developed a conceptual framework for legally compliant and meaningful privacy control in the IoT. However, the principle of enhancing privacy through control has also experienced criticism. Kröger et al. [27], for example, postulate that individual privacy control, no matter how effective it is, can never be the solution as it notoriously ignores consequences for others and society at large. Therefore, they demand strong government regulations to protect users' privacy instead of focusing on control. Hartzog [21] even states that privacy control is harmful and illusionary as control options are limited and selected by the data collectors. Moreover, dark patterns nudge users to consent to the options desired by the companies. Yet, they also argue that control tools can still empower users as long as they exist in the right regulatory environment.

In smart homes, personal data gets collected in the most intimate spaces, and as such, privacy is subject to even higher societal and legal expectations [5, 30, 61]. As such, research developed control mechanisms to give users back autonomy over their data. As Apthorpe et al. [3], for example, found that sensitive information from smart homes can be revealed by analyzing internet traffic, they propose traffic shaping to mitigate such privacy risks. Luria et al. [33] compared a novel social robot for smart home control to more conventional techniques and found it to be a promising solution while facing usability issues. To facilitate control in assisted living spaces equipped with smart surveillance systems, Moncrieff et al. [43] created a framework to adjust the privacy level in a smart home automatically depending on the context using data hiding techniques. Similarly, Arabo et al. [4] proposed a framework to protect users' privacy in smart homes by defining privacy zones and dynamically generating policies. In the context of smart toys, McReynolds et al. [38] proposed that toys should communicate clearly that they are recording or provide a feature for children to control and listen to their own recordings. Lin and Bergmann [32] suggested auto-configuring smart home devices and introducing automatic updates to keep them up to date with the latest firmware. *While these mechanisms provide promising directions, they were envisioned and implemented by researchers without user input.*

In contrast, Yao et al. [59] followed a user-centered approach by conducting co-design studies with smart home users. They found that users designed different control mechanisms, such as increasing transparency and control of collected data, keeping data local, disconnecting devices from the internet, preventing data collection, introducing authentication methods for multi-user scenarios, and providing access control through different modes. Yao et al. [60] were the first to focus on the bystanders' perspective in smart homes explicitly. For this, they conducted co-design sessions with bystanders to elicit mechanisms that mitigate their privacy concerns. They extracted two categories: cooperative and bystander-centric mechanisms. Cooperative mechanisms enable negotiations about privacy preferences and asking for device control. On the other hand, bystander-centric mechanisms increase bystanders' awareness of nearby devices and provide control by limiting data collection and processing. *These findings shed light on smart home users' and bystanders' privacy control needs in smart environments and highlight the importance of integrating users in the design process. Our work expands this research thread through the explicit focus on tangible privacy control.*

2.3 Tangible Privacy

Tangible mechanisms have been proposed as a promising means to regain control over one's privacy [13, 39, 40]. Based on their findings from interviews with smart home bystanders, Ahmad et al. [1] introduced the concept of "tangible privacy" and argue that bystanders require tangible mechanisms to assess device states and privacy risks of smart device sensors. A sensor that follows the principles of tangible privacy must 1) have physical mechanisms to control the data collection and 2) provide unambiguous feedback on what data is being collected in the sensor's vicinity. Existing prototypes of tangible mechanisms allowing control over individual smart devices and sensors include a wearable to disable microphones in the user's vicinity [10], a hat to be placed over a smart speaker to prevent it from listening [53], a tangible and portable smart calendar only revealing sensitive appointments when placed in private locations [26], and a smart tangible webcam cover activated when the camera is not in use [14]. The latter represents a

simple example of an automated control mechanism for tangible privacy features. The tangibility of privacy control mechanisms is also echoed in the work of Chalhoub et al. [9], who relate the need for privacy measures to the physical location of smart devices. For example, one of the study participants stressed that they kept a smart device in the bathroom because the physical camera shutter assured their privacy.

The aforementioned prototypes target individual devices and sensors and mostly have to be manually leveraged. They can not provide system-level control, which is needed in increasingly complex smart home environments. In an effort to provide a central control unit, Rodriguez et al. [49] prototyped PriKey, a tangible 3D printed key allowing users to deactivate sensor groups for individual rooms. However, this prototype was again not developed employing a user-centered approach. As such, it is unclear whether it matches the users' expectations and requirements. *Prior work showed that tangible mechanisms are promising means to provide control in smart homes as they offer high assurance and certainty that a sensor is indeed deactivated. However, current approaches only target individual sensors or are envisioned by researchers without user input.*

2.4 Summary

As prior research found that device owners and bystanders in smart home environments are concerned about devices [29, 30, 58] and that different sensors raise different levels of concern [57], **we need to hand users granular control over smart devices.** Tangible mechanisms are especially promising to provide control as they offer high assurance and certainty that a sensor is indeed deactivated [1]. However, **current approaches only target individual sensors** (e.g., [10, 53]) **or are envisioned by researchers without user input** [49]. Therefore, we employ a user-centered approach to investigate tangible privacy-preserving mechanisms for future smart homes.

3 METHOD

We conducted three studies to gain encompassing insights into the needs and requirements of tangible privacy-preserving mechanisms for future smart homes. To this end, we employed a rich mix of methods. First, as we identified a lack of user integration into the design process of tangible mechanisms, we conducted a focus group with eight participants. We presented them with speculative artifacts for tangible granular control to gain general insights into their usefulness and acceptance. After that, we divided the participants into groups and conducted co-design activities where participants designed a central control unit and strategies for resolving conflicts around divergent privacy needs and desired smart home functionality. Second, we conducted a workshop on tangible privacy mechanisms with eight HCI conference attendees to supplement the user perspective with academic insights. Finally, we conducted a six-week in-the-wild study with six households and 12 participants to investigate how a tangible, static privacy dashboard is perceived in daily life and gain insights into how privacy negotiations manifest in the real world. Finally, we note that all interviews were conducted in German. We manually translated all quotes in this paper into English. See Figure 2 for a visualization of our method.

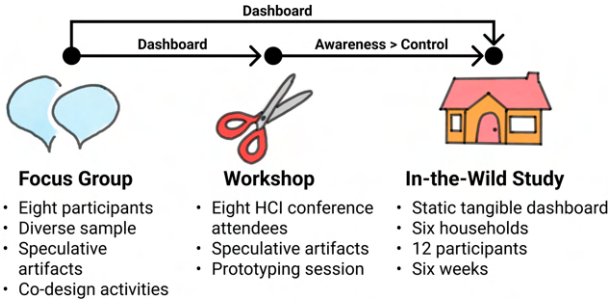

Figure 2: Overview of the overall research method. We ran three studies that differed regarding participant samples and study protocols. We envisioned privacy control requirements for future smart homes with a focus group and mapped design approaches with workshop participants of an HCI conference. We complement these findings with lived experiences from an in-the-wild deployment of a static privacy dashboard. The arrows depict how the key outcomes of the individual studies shaped the following study procedures.

Focus Shift. The findings of our individual studies shifted the focus of the following study procedures. While we first focused on controlling individual device capabilities through the SNOP artifacts, we deployed a central control hub in the form of a static dashboard that mapped floor plans and provided awareness instead of control in study III. One of our study I's key findings was the need for a central control hub, which both groups from the study I designed as a dashboard that mapped floor plans. We took these insights into our second study, where we directly tasked the workshop attendees with designing a central control hub. Here, our attendees focused on providing awareness instead of control. Finally, we deployed a static tangible dashboard that provided awareness by indicating the devices' locations in study III. We argue that the different foci of individual control, general control, visualization, and awareness, help advance the design space around tangible smart home privacy. Figure 2 gives an overview of how key findings shaped the following studies.

Data Analysis. We recorded all verbal interactions during the focus group and the conference workshop. Further, we conducted and recorded interviews with the participants from the in-the-wild study. We transcribed, annotated, and coded all verbal interactions and interviews through thematic analysis [7] using the software Atlas.ti. We performed a dedicated and independent analysis for each study, following the same general process. First, at least two researchers independently open-coded parts of the transcriptions. We reviewed, discussed, and refined those codes. We calculated the intercoder agreement for all three studies using Atlas.ti and Krippendorff's Cu-α [17]. We performed the agreement calculations on the complete data of study I as the findings substantially informed the following studies. For studies II and III, we used a random subset of about 20% of all transcribed data. We reached agreement values of 0.74 for study I, 0.86 for study II, and 0.84 for study III, meeting

agreement criteria typical for the community [20, 24, 41]. Based on the complete set of codes, we iteratively constructed code groups before defining overarching themes. For transparency and to enable future work, we provide the Atlas.ti intercoder agreement and code group reports for all three studies in the supplementary material.

4 STUDY I: FOCUS GROUP

We conducted a focus group with eight participants to gain insights into their tangible smart home control needs. We chose to run a focus group as we hoped to spark discussions by joining different experiences and expectations. In addition, we used speculative artifacts and co-design sessions to stimulate creativity and create concrete concepts.

4.1 Artifact Design

We used speculative design to create tangible mechanisms for smart home control. Speculative design is a method used to elicit the factors enabling a more desirable future – especially for technologies that do not yet exist and for which users lack hands-on experiences [15, 51]. We designed two speculative artifacts that can be put on sensory input devices. We refer to them as Snap-On Privacy (SNOP): (1) the manual SNOP frame, depicted in Figure 1b, is designed to block the camera of the Amazon Echo Show; and (2) a digitally controllable cover that fits onto common webcam models, shown in Figure 1c. Both artifacts are 3D printed.

4.1.1 Manual SNOP. We designed the static, manual SNOP frame to fit the Amazon Echo Show 5. This is a popular smart home device with a voice assistant and a video camera. As shown in Figure 1a, the Echo Show has a built-in tangible mechanism to block the camera in the form of a white marker. We designed the manual SNOP frame to investigate two aspects: (1) the role of visibility of tangible mechanisms and the users' interpretation thereof (i.e., the small white circle compared to the contrasting frame) and (2) the acceptance of manual privacy control processes.

4.1.2 Automated SNOP. The automated SNOP fits on common stand-alone computer webcams (see Figure 1c). At its core, the artifact features a common low-cost servo motor that can visibly move a yellow disk in front of, or away from, the camera. We chose to create a low-fidelity prototype that does not attempt to hide the servo and its connections in order to provoke honest reactions regarding the overall mechanism and control opportunities rather than initiate a discussion on design choices. The artifact is fully functional, and participants saw the shutter arm move into and away from the camera during the focus group.

4.2 Procedure

After we had settled on an appointment, we invited our participants to one of our university's meeting rooms. We welcomed the participants, asked them to sign an informed consent form, and started with an introduction round, where we exchanged general experiences about the benefits and convenience provided by smart home devices, followed by discussions around existing privacy concerns. After that, we presented our manual and automated SNOP artifacts. We asked our participants for general feedback, if they could imagine using it, and discussed the advantages and disadvantages of both. We then moved on to three individual co-design tasks for which we provided our participants with many different materials, including colorful paper and pens, scissors, and glue to foster their creativity. After each design task, we asked the groups to present their concepts to spark discussions around differing designs.

For the first task, we divided our participants into two groups of four and asked them to design a privacy control concept for a future smart home equipped with several smart home devices. We first introduced various concepts and ideas to our participants. Those concepts were: 1) The notions of central, device-level, and sensor-level control; 2) Different possible form factors, such as mobile apps, displays or tablets, and tangible control mechanisms; 3) Different symbols and metaphors that might be used, such as a padlock icon; and 4) possible conflicts in multi-user/bystander scenarios. We then instructed our participants to design control mechanisms that would satisfy their privacy needs in smart home environments. Apart from that, we intentionally left the task open to not bias our participants but to gain insights into their differing needs and expectations.

For the second task, we divided our participants into four groups of two and asked them to sketch a privacy profile containing their personal preferences regarding different sensors and functionalities. This task was motivated by prior work that already found that privacy needs strongly differ across individuals [22, 52, 58].

In the third design task, we asked our participants to design concepts to resolve conflicts caused by mismatching privacy profiles. Such conflicts can, for example, occur when two people are in favor of audio recordings while one is strictly against them. This task was again motivated by related work that reported negotiations around divergent privacy needs between bystanders and device owners [60]. We provide the study protocol and the artifacts generated in the design sessions in the supplementary material.

4.3 Participants

We aimed to recruit a set of participants that mostly had no technical background to gain insights into laypersons' control needs in smart homes. In total, we recruited eight participants using a university mailing list and selected them based on their demographics provided in a pre-screening questionnaire. The participants were between 21 and 54 years old ($M = 32.4$, $SD = 10.5$) and had different educational backgrounds: Most (3) in humanities, two in natural science, and one each in economics, care, and animal care. The focus group took two hours, and we compensated each participant with 20€. See Table 1 for an overview of our participants' demographics.

4.4 Findings

We followed the analysis process described previously, resulting in 193 individual codes, 18 code groups, and four overarching themes. Those four themes were (1) Smart Home Perceptions describing the benefits and disadvantages of smart home technology, including where participants' privacy concerns originate, (2) Device Control including concerns around unclear device states, increased trust in physical mechanisms, and discussions around manual versus automated control, (3) Smart Home Control describing the need for a central control hub in the form of a dashboard along with its desired properties, and (4) Mitigation of Privacy Needs

Table 1: Our participants' demographics: Their gender, age, highest educational degree, and their current occupation.

PID	Gender	Age	Education	Occupation
1	M	32	Sociology Studies	Scientific Employee
2	M	30	History Studies	Student
3	M	40	Nurse Training	Nurse
4	F	21	Economics Studies	Student
5	M	29	Sociology Studies	Student
6	M	54	Agricultural Apprenticeship	Animal Keeper
7	F	23	Media Informatics Studies	Student
8	M	30	Electrical and Information Technology Studies	Scientific Employee

characterizing the need of different roles and profiles to assign distinct rights and the potential for conflicts caused by diverging privacy needs.

4.4.1 Smart Home Perceptions. Here, several participants reflected on their experiences with smart homes and weighed the increased benefit and comfort provided by the devices against the increased complexity and emerging privacy concerns. Participants especially saw a benefit in automating tedious tasks, such as watering plants (P7) or closing windows when it rains (P1). Yet, participants also reported occasions where a smart device introduced unnecessary complexity, such as a smart oven that frequently updates, keeping the owner from cooking (P2), and discussed privacy concerns towards smart devices (P1, P2, P4, P6, P8). Overall, privacy concerns were most apparent towards devices with audio (P1, P2, P6, P7) or video capabilities (P2, P7, P8). Apart from that, privacy concerns varied strongly across individuals. P4, for example, considered location data especially concerning, while P7 did not see any danger in sharing this information. While participants generally agreed that who had access to their data influenced their concerns (P1, P6, P7, P8), some found familiarity to increase their concerns (P8), while others were more comfortable sharing data with strangers (P6). P6, for example, stated: *"I don't want my immediate neighborhood to know, but if some stranger knows, then I don't really care."* When asked what evoked their concern, P6 mentioned generally mistrusting technology, and P7 stated that having no control to limit or stop the data collection was the main reason for being concerned. In addition, she mentioned that many of her concerns were induced by society and peers: *"I only think about it because others always say that it is critical. And then I always think: Ok, maybe I should worry."*

4.4.2 Device Control. Before showing our SNOP artifacts, we presented the Echo Show with the activated integrated camera shutter and asked our participants whether they thought the device was presently able to record videos. Even though the camera was blocked, five of our eight participants thought it was able to film, which clearly emphasizes the inconspicuousness of the current mechanism. This provoked a general discussion about the often unclear state of smart devices. P6, for example, stated: *"I wouldn't even notice when it starts filming. Because most devices don't have a red light like, for example, laptops. There is no feedback."* P8 echoed this unclear recording state regarding smart TVs in hotel rooms. In contrast, participants saw a clear advantage in the SNOP frame as it provided haptic control and unambiguously made filming impossible (P2, P4, P5, P7). P5 additionally mentioned that such tangible, obtrusive mechanisms would provide increased *"comfort for guests. As they can be sure, I'm not filming."* Yet, our participants found the manual SNOP artifact cumbersome and did not think they would remove it again once attached (P2, P3, P4, P5, P8). Next, we presented the automated SNOP artifact. Overall, participants reacted positively, and P7 stated: *"That's extremely cool because you link the haptic control on which you can rely to automation, which makes it way less cumbersome."* Yet, participants also expressed concerns as they feared the automation could introduce privacy risks. P8, for example, said: *"then the question again is: can this somehow be controlled from the outside?"* In addition, our participants discussed how automation should work. Some wanted all sensors to be off by default (P2, P8) or preferred the sensors to be coupled to an intention, such as performing a video call (P7, P8). These initial discussions already surfaced the complexity involved in automating control on the sensor level.

4.4.3 Smart Home Control. Both groups designed a central control hub as they saw it as a crucial requirement to bundle control in a central place for increasingly complex smart home environments, where it might be easy to lose the overview (P4, P8). In addition, both groups independently designed a dashboard with a floor plan to map the device locations, see Figure 3. P4 suggested using color coding to mark a device's activity status. Moreover, while P6 and P8 saw it as the minimum feature to convey which sensors a device leverages, P6 gave visitors the option to deactivate the sensors that made them uncomfortable. Other suggested features included a handbook to explain all features of a smart device to visitors (P4) and a logging feature to investigate at which times a device has been active (P7). For the placement of the dashboard, both groups agreed to place it in *"the most visible position"* (P2) so that visitors immediately become aware of it. P7 suggested placing it right next to the entry door, and P8 proposed placing it in the hallway. In terms of the level of control, both groups agreed to have an "all devices off" button. However, to provide more granularity and address individual rooms' sensitivity, P8 suggested adding a button to turn off all devices in a specific room or by a specific sensor type. P4 proposed dividing smart devices into "privacy-concerning" and "non-concerning" devices and only allowing control over concerning ones. Along those lines, one group introduced different presets according to individual privacy preferences. During the presentation, the other group agreed that this was a great idea as it would reduce the configuration complexity. Notably, these discussions during the presentation of the first task already surfaced issues around privacy preferences and conflict resolution that relate to our scheduled follow-up design tasks. However, we note that the participants ultimately self-motivated these topics without any influence from our side. Apart from the dashboard, both groups designed a supplementary mobile version to make it possible to *"control the devices without having to run to the hallway all the time"* (P7).

4.4.4 Mitigation of Privacy Needs. In the second and third design tasks, we asked participants to design a personal privacy profile and strategies to resolve conflicts around diverging privacy needs. The idea of a privacy profile had already come up during the dashboard

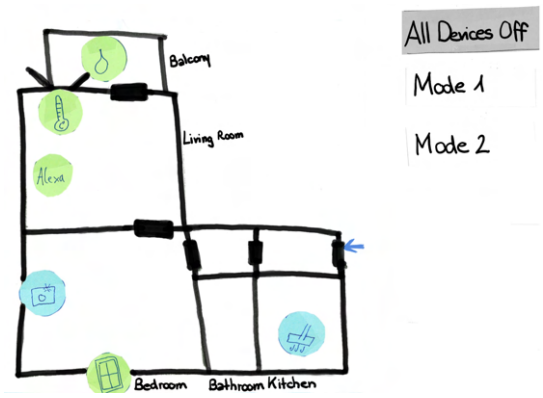

Figure 3: The design for a tangible smart home control dashboard of one group of our focus group. It shows an apartment's floor plan with the smart devices' locations. To the right is an "All Devices Off" button to switch all smart devices off at once and two "Mode" buttons, which can be programmed with individual privacy settings.

design, where participants discussed having a personal privacy profile on one's phone, which syncs with smart home dashboards to adjust settings automatically (P2, P4, P7). When designing the privacy profiles, trust was a major topic: Both groups agreed that people should have different roles – the closer the relationship, the more rights they should get in controlling the smart devices. Here, P8 explains that while close friends get to control devices directly, acquaintances only see which devices are present and whether they are currently active. Yet, P2 and P7 agreed that having such different profiles might lead to socially awkward situations, for example, when one might *"get downgraded from close friend to just friend"* (P2) and, thus, loses rights in controlling devices. When it comes to resolving conflicts around diverging privacy needs, most participants agreed that technology could serve as a trigger to surface them or make suggestions for solving them (P1, P3, P6, P8). Such suggestions could, for example, be democratic and recommend implementing the most frequently desired preferences (P2, P5). Yet, even though technology can make suggestions, in the end, solving conflicts remains a human process that has to happen offline, as P6 explains: *"We have come to the conclusion that verbal communication is the only way out"* (P6).

4.5 Summary

Overall, our participants reacted positively to the SNOP artifacts and reported having high trust in the physical mechanism as it provided indisputable certainty that a sensor was inactive. However, they also found it cumbersome as it has to be manually attached to each sensor. In addition, this mechanism would scale badly for the increasing number of smart devices in future smart homes. A remedy for that would be the automated SNOP artifact, providing the certainty of a tangible mechanism combined with automatic control. While participants generally liked the idea, they also feared that the artifact might introduce new concerns as the ability for automatic control could be abused and, thus, represent a security risk. In addition, it is not clear how these artifacts should be controlled. In the design task, participants decided to create a central control hub in the form of a dashboard that mapped a floor plan indicating the smart devices' location and activity status. While participants agreed that the dashboard should provide awareness of the presence of devices, they had differing opinions on who should be able to exert control. In general, the participants agreed that control must be reflected in the level of personal trust. This was also reflected when discussing privacy profiles; participants created different roles with differing rights. Overall, participants agreed that technology can trigger surface conflicts around diverging privacy needs and can make suggestions to resolve such conflicts. However, our participants also agreed that conflict resolution remains a human process that needs to happen offline.

5 STUDY II: HCI CONFERENCE WORKSHOP

To supplement the findings from the focus group and gain insights from an academic perspective, we conducted a workshop with eight HCI conference attendees on the topic of tangible privacy control. We again used the SNOP artifacts from the first round in combination with co-design activities to develop concepts.

5.1 Procedure

We asked our participants to sign an informed consent form and started with a brainstorming session, asking participants to document their thoughts about perceived benefits and concerns of smart home devices, what information they would like to receive (e.g., which devices, what capabilities, possible consequences), and which level of control they would like to exert in smart home environments. As our participants presented their thoughts, we clustered them on a pinboard and compared and discussed them. Next, we presented prototypes for tangible control in smart homes: the two SNOP artifacts from the focus group as examples of granular tangible control and, as this was an important finding from the first focus group, two examples of centralized control. We presented a dashboard with a floor plan indicating the device location and sensor capabilities, as suggested by our participants from the focus group and the PriKey from related work [49] as they represent two rather different concepts for centralized tangible control. We then asked for general thoughts on the presented concepts' perceived benefits and shortcomings. The workshop's final task was a prototyping session for which we separated the participants into two groups. We again handed them various materials, such as colored pens, paper, scissors, and glue, and asked them to prototype their own version of a tangible privacy-preserving control mechanism. We asked them to consider different levels of control, form factors, materials, and possibly conflicting privacy preferences. After both groups had finished their prototypes, they presented them to the other group and discussed and compared their ideas. We provide the study protocol and the artifacts generated in the prototyping session in the supplementary material.

5.2 Participants

We conducted the workshop at an HCI conference where it was advertised as focusing on *tangible interaction*. Overall, eight attendees participated who were between 25 and 35 years old (M = 29.9,

SD = 3.5). Six held a master's and two a bachelor's degree. Most (6) were Ph.D. and two undergrad students.

5.3 Findings

Our analysis led to 59 individual codes, eight code groups, and the following three overarching themes: (1) Analog versus Digital, describing our participants' notions around analog mechanisms providing higher security in contrast to the comfort provided by digital solutions, (2) Awareness over Manipulation, conveying why our participants decided to rather raise awareness instead of providing control and how they plan to achieve this, and (3) Design Principles containing general considerations around open source software and standardization.

5.3.1 Analog versus Digital. This theme emerged from our participants' smart home control designs. Both groups designed a tangible, portable artifact to store one's privacy profile. However, while one group designed a digital token as a keychain that can be docked to a smart home dashboard to analyze preferences automatically, the second group completely dispensed with digital methods on the users' side. Instead, they designed a punch card that can be inserted into a machine before a smart home's entrance to again, sync their preferences and visualize where they differ from the smart home environment. E1 explained that they opted for non-digital methods as *"another wireless chip that connects to the wifi and syncs with the smartphone"* would introduce a new attack surface. However, a clear disadvantage of this approach is that, as soon as preferences change, the punch card can not be overwritten, but a new one has to be created (E2). As a possible solution, E2 suggested using a diskette instead. Even though this group designed a dashboard that reads the information encoded on the punch card, they discussed that this again introduces privacy concerns as the dashboard can keep track of privacy preferences. In contrast, the other group emphasized that their digital token can easily be configured using a smartphone app – a comfort level not achievable with analog methods.

5.3.2 Awareness over Manipulation. Our participants discussed the level of control visitors of smart homes should be able to exert. Both groups did not allow users to control devices directly but decided to merely provide awareness. For that, both groups designed their dashboards in the form of a hub that syncs with the visitors' digital or analog profiles and visualizes where preferences clash. E6 described that as a form of *"entry-level privacy"* as it shows users which devices are present and, thus, gives them the power to decide if they want to expose themselves to possible privacy risks. This way, there would also be no option to deactivate *"possibly vital devices"* (E6). In cases where the central control hub might surface a conflict of personal privacy preferences in contrast to the settings of the smart home environment, both groups resorted to offline conflict resolution strategies through verbal communication. While one group designed the privacy profiles in a way that users can declare with which sensors and devices they are comfortable, the other group went away from raw sensors to concrete risks. This way, the group aimed to provide even more awareness, as it might be hard for users to assess the concrete risks posed by a device or sensor (E3). To provide this awareness as early as possible, one group suggested placing the hub directly at the entrance, while the other group would even place it in front of the door, for example, next to the letterbox, as even the doorbell might already be a smart device and thus, collect sensitive information.

5.3.3 Design Principles. Our participants also made design considerations on a more holistic level. One important point here was the notion of open-source software. The group with the analog punch card saw it as vital to provide insights into the source code to ensure that the dashboard, supposed to enable more privacy, does not become a privacy risk (E2). Moreover, E3 discussed that people having strong privacy concerns are often also more resistant to engaging with technology. Thus, making software open source could increase their general technology acceptance. In addition, both groups agreed that whatever approach gets implemented has to be a standardized solution to be effective, meaning that each privacy profile fits with each smart home privacy dashboard.

5.4 Summary

The workshop participants discussed intriguing new aspects around dispensing digital methods when storing privacy profiles, as this would prevent digital attacks. However, an important tradeoff here is that the increased level of privacy would come at the cost of comfort provided by digital methods. When designing the tangible smart home control hub, both groups decided to increase awareness instead of providing control. They saw it as a mild intervention to give users enough information to decide if they want to enter a smart home consciously. In terms of how this information should be conveyed, the workshop participants explained the benefits of conveying the concrete risks posed by a sensor, as those are often unclear to users. On a more holistic level, they discussed the benefits of making privacy-enhancing software open-source as it might increase users' trust. In addition, both groups agreed that standardized privacy profiles in combination with smart home dashboards are necessary to provide real merit.

6 STUDY III: DASHBOARD IN-THE-WILD

We conducted a longitudinal in-the-wild study with six households over six weeks. We equipped all households with static tangible smart home dashboards to investigate visitors' reactions and gain insights into real-world negotiations around privacy preferences. In addition, we did pre- and post-study interviews and provided our participants with online diaries to track all interactions the dashboard sparked.

6.1 Study Artifact

We made several design choices aligned with the findings from the focus group and the conference workshop: (1) we decided to focus on awareness instead of control as this was recognized as the important first step in the focus group and workshop; (2) we designed dashboards mapping floor plans that indicated the smart devices' locations as this was the general form of representation used by both groups of our focus group; (3) in addition to the type of device, we also marked the sensors as this was desired by both groups of the focus group and one workshop group; and (4) we marked whether a device is connected to the internet or only local network as a connection to the internet was a major trigger for privacy concerns in our focus group.

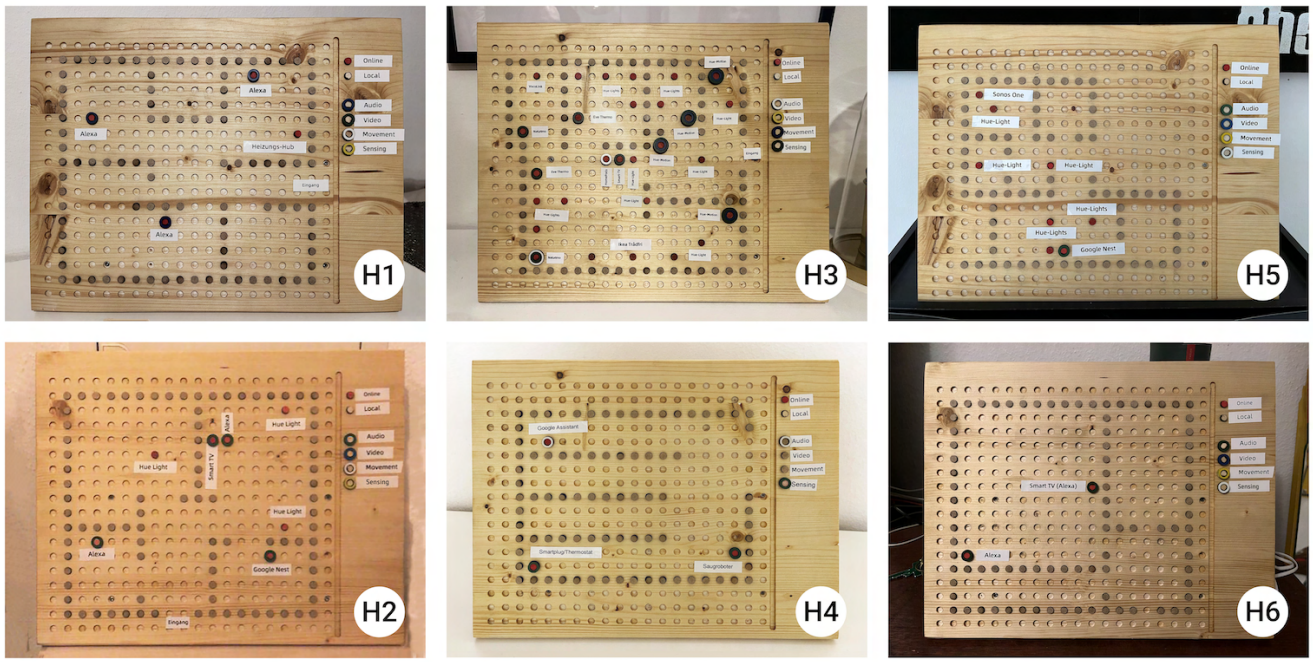

Figure 4: All tangible, static smart home dashboards as we configured and deployed them in our six participating households.

Based on these design choices, and particularly the focus on awareness and human interaction, we built a static wooden dashboard with a 20×20 grid that fits wooden plugs. We created two types of plugs: (1) brown plugs to mark the apartment's floor plan and (2) red or white plugs to mark the smart devices. We used red plugs for devices connected to the internet and white ones for devices only connected to the local network. In addition, we created different colored rings in different sizes to mark a device's sensors. The rings had different sizes so that multiple rings fit on a device to visualize multiple capabilities. We had the ability to visualize four different sensors, namely audio, video, movement, and general sensing (e.g., temperature or ambient noise). We chose these sensors as prior work found them to raise the biggest privacy concerns [57]. A legend to the right of the dashboard explained the meaning of the different colored pins and rings. See Figure 1d for a close-up of the static dashboard.

6.2 Procedure

First, the participants signed an informed consent form, and we set up the dashboard together. We advised the participants to use the plugs to map their floor plans and mark their smart home devices. When they had finished the setup, we placed the dashboard near the entrance, aligned with the suggestions from our focus group and workshop participants. Figure 4 shows all configured and deployed dashboards.

After the setup, we conducted short semi-structured interviews about our participants' general knowledge of smart home privacy, previous conversations with visitors about their smart home setups, and concerns about different data types and manufacturers. After the interview, we explained the procedure for the next six weeks. We instructed the participants to keep a diary of all interactions that occurred in response to the smart home dashboard. To avoid memory bias, we tasked participants to either take notes during the interactions or submit their experiences immediately. We collected the entries using an online form, which included the following questions: the time of interaction, the number of people involved, the relationship with the involved persons, and the content and outcome of the interaction.

After six weeks, we met again for another semi-structured interview. The focus of the second interview was the participants' interactions sparked by the dashboard and their general experiences using the dashboard over the last six weeks. Therefore, we read all diary entries before the interview to document the aspects we wanted to discuss in depth.

6.3 Participants

We recruited the participants using convenience sampling, our university's mailing list, and social media channels. To be eligible for our study, participants had to match our inclusion criteria which were 1) had to own at least two smart home devices and 2) expected a few visitors during the six-week study duration. Overall, we recruited six households with 12 inhabitants. For a detailed overview of the participating households, see Table 2. We did pre- and post-study interviews and asked participants to keep a diary of every interaction caused by the dashboard. In sum, we received 23 diary entries ($M = 3.8$). During the study period, our participants had 31 visitors. H1 and H2 each had six, H3 five, H4 seven, H5 four, and H6

Table 2: Overview of the participating households, including their number of smart devices, the device types, whether they are the device owner or a bystander, their age, and occupation. The main study participant has an ID with a "P," whereas people living in the same household have a "B."

HID	#	Devices	PID	Role	Age	Occupation
H1	4	Alexa (x3), Smart heating control	P1	Device owner	30-35	Chef
H2	7	Alexa (x2), Hue Light (x3), Smart TV, Google Nest	P2	Device owner	25-30	Student
			B1	Device owner	30-35	Real Estate Expert
H3	26	VocoLink, NetAtmo (x2), EveThermo (x2), Homepod (x2), Ikea Tradfri, Smart TV, Hue Lights (x13), Hue Motion (x4)	P3	Device owner	25-30	Student
			B2	Device owner	25-30	Nurse
H4	3	Smart Plug/Thermostat, Robotic Vacuum Cleaner, Google Assistant	P4	Device owner	20-25	Student
			B3	Bystander	40-45	Baker
			B4	Bystander	50-55	Chemical Technician
			B5	Bystander	10-15	Student
			B6	Bystander	15-20	Student
H5	8	Hue lights (x6), Sonos One, Google Nest	P5	Device owner	30-35	Editorial Manager
H6	2	Smart TV, Alexa	P6	Device owner	20-25	Backend Developer

three visitors. We estimated the active time required for the study at 3.5 hours and compensated participants with 35€.

6.4 Findings

Our analysis led to a total of 103 individual codes, 13 code groups, and three themes: (1) Functionality, describing how the dashboard performed in everyday use along with its advantages and shortcomings, (2) Reactions, illustrating how bystanders reacted to the dashboards and which actions they took to protect their privacy and (3) Acceptance, including notions around resignations and factors influencing their privacy concern, such as sensors and locations.

6.4.1 Functionality. A major reason for using a tangible dashboard placed prominently near the entrance was the assumption that it would attract visitors' attention. It performed well in this regard since most visitors touched upon the dashboard right away or at some point during their visit. Moreover, participants considered the dashboard much more noticeable than a digital solution, as P3 stated: *"If it'd been only an app, I'm sure I'd have forgotten about it. I think it's great that it's so present."*

However, very few visitors recognized the dashboard's purpose right away or were confused by the content. P3 stated: *"It's not self-explanatory, one needs a person to explain things."* Visitors of H2 and H4 misunderstood the dashboard for a game or toy. Moreover, every household reported visitors having trouble recognizing the floor plan. While one participant assumed that people might not have recognized it because the plug system was not concise enough (P3), P6 supposed it was due to his apartment having no distinct features in terms of layout. As a solution, P4 suggested adding a headline to the floor plan. In addition, P2 mentioned that their visitors did not comprehend what *online* and *local* meant, and visitors of both H2 and H5 struggled with the term *sensing*. However, every participant added that these problems were quickly resolved by explaining the dashboard. Contrary to all those statements, P5 reported that every visitor understood the content right away except for the term *sensing*.

Most participants stated not having considered informing visitors about their smart home setups before the study and that the dashboard provoked that thought (P2, P3, P5, P6). All participants agreed that the dashboard raised awareness for visitors and themselves and helped them keep track of their smart home setups. P2, for example, explained that one gets so used to the devices that they are easily forgotten:

> *"It also creates awareness for oneself that these devices are there. You forget that at some point. When they're new, you still think to yourself, "Okay, they're here, they're listening," and that sort of thing, and after a while, you just become completely numb to it."*

P3 also considered the dashboard helpful in reminding them where exactly devices are located. P1 said that merely walking by the dashboard led him to think, *"maybe someone is really listening right now"*. P6 said that, although the study did not change his general perception of smart home devices, since he was already quite careful, he did some research afterward and plans to be even more careful when it comes to cheap devices.

While all participants liked the physicality of the dashboard, considered it helpful in communicating their smart home setups, and agreed that it generally raised awareness for themselves and visitors, they reflected on possible future enhancements. P1 and P2 discussed that it would increase engagement if people could interact with the dashboard and not just look at it, for example, by turning devices off (P3, P4, P5). Participants also suggested that the board provide concise summaries of privacy policies and security risks or send update notifications (P2, P5, P6). P5 stated that he would like

the comfort of having a board that enabled central control over all smart home devices.

6.4.2 Reactions. All households reported that the dashboard caused numerous conversations about smart home privacy. In response to noticing the number of smart devices in P2's home, their sister started a conversation about sensitive information that can be derived from smart home data and emphasized that she would never trade her privacy for comfort. She also asked P2 about the exact functionality and sensors of devices she did not know yet. Similarly, P6 reported how the dashboard sparked a discussion with their partner about the amounts of data collected by big companies, which resulted in them speculating about what was being done with the data. The dashboard even led to visitors testing from what distance a smart assistant still responds to voice commands, making them noticeably concerned as they realized that most assistants worked throughout the entire apartment (P2, P3).

Additionally, the dashboard raised awareness about the number and presence of smart devices and their capabilities. Several visitors of H3 were stunned by the sheer number of smart devices and asked why they were necessary. Moreover, a friend of P6 was *"visibly shocked after learning about the possibility of third parties listening to all conversations recorded through a smart device"*. This increased awareness led to several visitors expressing their discomfort with smart home devices, and a friend of P6 even directly asked to switch a device off. Other visitors still expressed discomfort while not directly asking to turn a device off. A friend of P4, for example, mentioned not being happy about smart devices capturing temperature and visual information, and a friend of P4's mother even reacted *"fearful"* and expressed that *"she does not want smart devices to capture any information"*. A friend of P5 clearly expressed being uncomfortable with the smart devices but considered *"the friendship more important"* and, thus, avoided the confrontation. Yet, several visitors explicitly mentioned being thankful to the dashboard for informing them about data being captured since, as long as they knew about it, they were comfortable with it (P2, P4).

6.4.3 Acceptance. Several visitors showed signs of resignation. For instance, visitors and household members of H4 did not like the idea of sensors capturing data but did not consider their data sensitive or important enough to be worth protecting. A visitor of H5 expressed privacy concerns regarding audio recordings as well as little trust in manufacturers but argued that, as a visitor, their information *"gets lost in the crowd."* In addition, several visitors of H1 and H5 explicitly stated to value the comfort provided by smart home devices more than their privacy, especially regarding smart lights and voice assistants.

It also became apparent that a number of visitors accepted the smart environment due to familiarity with either the environment (i.e., being in the home of a trusted person) or smart homes in general. For example, several visitors reported being comfortable using smart home devices as they provided similar functionality as modern smartphones (H1, H2), and visitors of H1, H2, and H5 did not consider smart home devices concerning as they owned several themselves.

Visitors found video recording most concerning (H2, H3, H5) and explicitly stated that they would oppose being captured by cameras. However, they accepted video recordings for special use cases, such as baby monitors (H2, P5) or security cameras at the front door (H2, P3, P4, P6). For a visitor of H2, the most important factor was where the data gets stored and who can access it, and P5 mentioned always weighing the privacy risks against the use case.

Several participants considered certain areas in their apartments more sensitive or even off-limits for data recordings. For video and sometimes even audio, rooms like the bedroom (P1, P4), bathroom (H2, P2, P3, P6), and living room (P3) were perceived as most concerning. P2's sister said she would not like a smart assistant in her bathroom when learning about P2's Alexa being placed in the bathroom. Yet, visitors of H5 did not consider the placement of a smart device important as they considered the whole apartment a private space.

6.5 Summary

Participants and visitors agreed that a tangible dashboard placed prominently at the entrance grabs attention – more than a digital solution. Yet, some participants had trouble understanding the dashboard at first. However, as soon as the owner explained it to them, they found it helpful and engaged in discussions about smart home privacy. Overall, it became apparent that the dashboard raised awareness of the devices' presence and capabilities for the device owners and visitors. Moreover, the dashboard led to several visitors expressing discomfort, asking detailed questions about the smart devices, and even testing their capabilities. Yet, visitors only rarely asked to turn devices off because they did not consider their data sensitive or wanted to avoid social conflict. These findings highlight the value of closely studying human interaction and negotiation around awareness as provoked by the static dashboard.

7 DISCUSSION

We mapped the needs and requirements involved in the design of privacy-preserving future smart homes through a rich mix of methods that included a focus group, a workshop at an HCI conference, and an in-the-wild prototype deployment with corresponding interviews and diary entries. Our focus on tangible privacy artifacts is in line with current research challenges [1] that pose open questions related to their use in increasingly complex smart homes. Based on our findings, we advocate for control features across the wider spectrum of tangible privacy, contrast privacy awareness with control, and discuss these implications through the lenses of inclusive privacy.

7.1 Enabling Control Across the Tangible Privacy Spectrum

Currently, smart devices are immensely limited in terms of control: they mostly only have one option – turning them off or unplugging them. Yet, this starkly contrasts users' diverging privacy concerns regarding different sensor types [57]. While users might reject video, they might still be comfortable with audio recordings. This was also reflected among our users: the focus group participants enabled the deactivation of individual sensors in their privacy designs, and multiple participants and visitors in our in-the-wild study reflected on their diverging comfort levels regarding individual sensors. Therefore, **we call manufacturers to provide control over individual sensors through a standardized system.** As such,

granular control can even increase device acceptance as users can adjust them to their privacy needs. While such granular control in the devices' firmware is an absolute must and comparably easy to realize, **there is also a need to provide tangible privacy mechanisms that instill trust and signal sensor status whenever feasible.** This was especially reflected in our focus group, where participants discussed how the often unclear device status of smart devices increased their discomfort as they, for example, were unaware when a device was currently able to film. Currently, such tangible metaphors mainly exist for cameras in the form of a physical camera shutter. Yet, there is current research investigating how such metaphors can be extended, for example, in the form of a physical hat to disable audio in a voice assistant [53]. Thus, we call for future research to investigate **how sensors other than video cameras can be matched to universally interpretable physical metaphors**.

However, the need for physical mechanisms was not only reflected at the sensor level. Our participants in the focus group and the workshop designed a tangible central control hub as they considered it more noticeable than a digital solution. Moreover, our workshop participants also designed portable tangible privacy profiles, either in the form of a digital token acting as a keychain or even purely analog in the form of a punchcard. This clearly shows the **need for tangible mechanisms, not only on the sensor level but across the entire tangible privacy spectrum.**

7.2 Designing for Awareness and Control

It became very apparent that the static tangible smart home dashboard, placed prominently near the entrance, led to a significant awareness increase for device owners and visitors. Moreover, the tangible device became a continuous point for reflection with visitors who repeatedly questioned why the devices were necessary or showcased their privacy-compromising capabilities by, for example, testing the range of voice assistants. This way, dashboards constantly reminded the device owners of their devices' presence and the ongoing data collection – something participants had already reported getting lost over time as the devices became familiar and, thus, blended into the environment. However, being conscious about possibly privacy-comprising technology is important as prior work already showed how users tend to only engage once with privacy settings and then forget about it [44]. However, contexts and personal preferences change and, as such, individual privacy needs. Therefore, **tangible privacy dashboards can serve as a central point for continuous privacy reflections and, thus, better privacy protection.** Yet, we also note that digital counterparts might provide useful additional information, as findings in the context of SaferHome, a physical-digital privacy framework, showed [56].

Upon interacting with the dashboard, several visitors expressed their discomfort with being exposed to smart home devices. Yet, only one visitor directly asked to switch a device off. When asked, visitors reported that they either did not consider their data protection-worthy due to their role as a visitor or wanted to avoid confrontation. This shows bystanders' internal conflicts of wanting to protect their privacy while acting in a socially desirable way. Yet, several participants stated being thankful for the dashboard's presence as it notified them about the ongoing data collection, which, in turn, put them in control over which information they were comfortable sharing. Moreover, our focus group participants agreed with our workshop participants that, while technology can surface privacy conflicts, resolving them remains a human process that has to happen offline. This shows **that future systems have to be designed for both awareness and control rather than focusing on a single dimension.** Along these lines, awareness becomes an enabler for smart home bystanders that allow them to make informed decisions about their engagement and privacy negotiations with device owners while considering additional factors like personal relationship and social circumstances surrounding the particular visit. Future dashboard iterations might even provide direct control if the host and device owner decides to add such features. Direct device control through the dashboard was envisioned by several participants in our in-the-wild study (see Study III, Functionality). Homeowners are likely to make such decisions based on their willingness to share control, the value that they assign to their smart devices, and their willingness to enter into social interactions and negotiations about their smart home setup.

7.3 Designing with Tangibles Means Designing for Inclusive Privacy

Tangible privacy control mechanisms are not restricted purely to the academic world. Indeed, there are several examples of tangible privacy control mechanisms in everyday life. Think, for example, stickers or attachments placed on laptop webcams or smartphone cameras or even curtains used to shield private spaces. Such tangible mechanisms are inherently inclusive as they provide undisputable certainty that a sensor, capability, or device is deactivated without requiring a deeper technical understanding. Moreover, the user does not need to be especially trusting in technology; when a physical object covers a camera, it is obvious that it cannot film. Hence, transferring familiar real-world metaphors to the digital world can empower people across all backgrounds to regain autonomy over their privacy. However, at the moment, we lack a comprehensive understanding of how to design for tangible control. This work helps advance the design space around tangible mechanisms by highlighting different facets and especially recognizing the importance of human interactions triggered by tangible privacy control mechanisms.

Being inclusive means providing pathways for participation across diverse societal groups. In the context of privacy, inclusiveness relates, among others, to *"under-served populations such as children, older adults, people with disabilities, and people from non-Western developing countries to effectively protect their security and privacy"* [54]. Notably, our findings surface concerns regarding the inclusiveness of future smart home privacy tools. For example, participants in the focus group study argued for a simple and static tangible privacy dashboard to **provide every visitor with an equal opportunity for building awareness and entering into an informed discussion** with the host or device owner. This will profit particularly those who do not have the necessary resources, such as money or knowledge, to engage through the latest technologies and applications.

The key principle behind the static dashboard, motivated and designed by our focus group participants, and evaluated in the wild across six households, relates to its intuitive nature and ease of interpretation. In terms of functionality and comfort, it contrasts with more advanced solutions like a mobile companion that some focus group participants envisioned. While these promise increased comfort, they fail to match inclusive privacy needs, as discussed previously. Yet, we also argue that the acceptance of future systems for privacy awareness will need to consider potential conflicts with users' perceived key advantage of smart homes: the heightened level of comfort. Therefore, future systems will need to **strike a balance between privacy inclusiveness and device owners' expectations around smart home control**. In this context, static tangible privacy dashboards might represent a type of **least common denominator accessible and understandable to everyone**. Based on findings from our in-the-wild study (see *Functionality*), we further note, however, that tangible artifacts might introduce interpretation challenges that reflect their analog nature. For example, participants suggested adding a dashboard headline and increasing the contrast between the plugs and the dashboard surface. Digital applications would likely prompt developers to set a descriptive window title. Designers and developers would also likely make use of validated templates or color schemes that are grounded in user experience design principles. As our iterative dashboard design shows, the same must not necessarily be true in analog and tangible devices that offer a higher degree of design freedom. Here, skipping a headline field will not result in the creation of empty space. **Transferring selected basic validated digital design concepts** into tangible artifacts will help make them suitable for inclusiveness, rather than actually excluding individuals through visual and interpretation barriers.

Such reflections around the acceptance of future devices and artifacts ultimately hook into wider discussions around privacy regulations. Given the documented divide between static tangible smart home artifacts that foster awareness and their mobile digital counterparts, we perceive the need to **spark a larger discussion across the wider society and lawmakers regarding future regulations**. We argue that these discussions should place particular emphasis on physical mechanisms and devices, as we find that **tangibility acts as a driver for inclusive privacy** across the design spectrum: they provide clear status information and control options on a device sensor level, allow translating privacy preferences into tangible tokens, and provide awareness related to the entire smart home through dedicated surfaces.

Concluding, we argue to further explore **tangibility as a driver for privacy inclusiveness**. In particular, we emphasize matching tangible mechanisms and devices across the tangible privacy spectrum to suitable interaction paradigms. The work of Mehta et al. [40] provides a valuable frame of reference for this research thread. The authors described *Privacy Care*, a tangible interaction framework for privacy management that addresses research at the intersection between privacy management, tangible computing, and embodied interaction. While the framework, rooted in literature, provides a rather high-level reference on tangible privacy that does not specifically consider smart homes and the needs of bystanders, it describes interaction tenets that closely relate to our findings. In particular, their notion of *Direct* interaction highlights the naturalness and directness of tangible interaction and advocates for the use of suitable physical metaphors. This relates closely to our findings that motivate research into the development of metaphors on a device sensor level. Along these lines, we expect that research across the spectrum of tangible privacy will not only result in the development and evaluation of mechanisms and devices that address challenges at the intersection between individual device sensors and smart home control hubs; rather, it will contribute to a refined understanding of frameworks like Privacy Care through lived experiences and further the development of inclusive privacy that ensures fair participation across the society in shaping our most personal and sensitive spaces.

7.4 Limitations and Future Work

At the moment, our dashboard is restricted to two dimensions and specific sensor types (i.e., audio, video, motion, and general sensing capabilities). We chose these sensors as previous work found them to be the most concerning [57]. Yet, we expect an increasing penetration of homes with smart devices that might have completely new capabilities; thus, this selected sub-set should not be seen as static but as a solid starting point to be expanded whenever necessary. Regarding the two dimensions, multiple stories could, for example, be represented by increasing the dashboard's size and placing the individual stories below or next to each other, just as it is done for multi-story paper floor plans.

We decided to implement the dashboard as a wooden board with a grid, pins and rings to visualize the rooms, devices, and capabilities. Another visualization could, for example, have been a drawing or a 3D rendering. However, we decided on a tangible wooden board as we wanted the participants to engage with their own smart home setup extensively. In contrast to a drawing, the wooden dashboard guarantees a certain consistency across multiple households. In addition, even though some visitors had trouble recognizing the floor plans at first, the dashboard's unusual form factor and appearance led to visitors noticing it and engaging in discussions as they were curious about its purpose. Yet, it would be interesting for future work to explore and compare the advantages and disadvantages of different form factors.

While we recruited participants with differing backgrounds to account for individual preferences and expectations and supplemented users' insights with UX designers' views, our sample solely focuses on a German-speaking Western population. This sample focus needs to be acknowledged, as Germans are characterized as particularly privacy-sensitive [50]. Especially the discussions around how to resolve conflicting privacy needs and who should be able to exert control over smart devices might be skewed by these perceptions. Thus, we argue for future research across diverse populations. In this context, we further note the sample size within each study as a limitation for the generalizability of our findings. Nevertheless, we stress that the focus group and in-the-wild studies profited from sampling participants across wider educational and age spectra.

Further, we note that research is needed across all stages of tangible privacy. On the device sensor level, our speculative artifacts focused on video cameras, as most people understand and know

physical interventions (i.e., camera shutters). And while we uncovered the need to provide similar transparent control mechanisms for diverse sensor types, research still needs to better understand corresponding suitable metaphors that transparently communicate their status across all societal groups. Related to tangible tokens that store privacy preferences, we note that further requirements research is needed to understand this design space. Finally, on the smart home level, we prototyped and deployed a static privacy dashboard that aligns with the designs of our focus group participants. While we note the limited interaction possibilities with this dashboard as a limitation, we emphasize the value of first introducing and studying a tangible artifact that allows us to understand better how awareness is built, possibly internalized, and echoed in interactions and negotiations with device owners. Based on our findings, we envision further research into tangible privacy dashboards that allow us to manipulate smart home environments. However, we emphasize the need to consider the potential ethical ramifications that result from such a shared control device in the study design and the communication with study participants and their visitors.

8 CONCLUSION

We reported findings from three studies designed to investigate privacy control in increasingly complex future smart homes. Our research explicitly focused on needs and requirements around tangible privacy mechanisms and the inclusion of smart home bystanders. To this end, we ran a focus group with speculative design artifacts (Study I), a workshop at an HCI conference (Study II), and an in-the-wild deployment study of a static privacy dashboard across six households with interviews and diary entries (Study III). We found that while some users expect future tangible tools to provide automated smart home interventions, most saw tangible mechanisms as a trigger for personal interaction, negotiation, and conflict resolution. This is echoed in our understanding that future systems need to be designed for both awareness and control, rather than focusing on a single design dimension. We further note that while our research initially focused on the tangibility of mechanisms on the smart device sensor level (e.g., cameras, microphones, and motion sensors), we found that tangible devices are expected to carry similar value around transparency and ease of manipulation in various forms, including carry-on tokens that store privacy preferences, and entrance hall dashboards that provide a device overview. We referred to this as the spectrum of tangible privacy and discussed its characteristics through the lenses of inclusive privacy. While much future research has to investigate tangible privacy interventions across this spectrum systematically, we argue that it will help to address challenges around awareness and control in increasingly complex smart homes.

REFERENCES

[1] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2020. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW2, Article 116 (oct 2020), 28 pages. https://doi.org/10.1145/3415187

[2] Noah Apthorpe, Dillon Reisman, and Nick Feamster. 2016. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *Workshop on Data and Algorithmic Transparency* (2016).

[3] Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster. 2017. Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic. *arXiv preprint arXiv:1708.05044* (2017).

[4] Abdullahi Arabo, Ian Brown, and Fadi El-Moussa. 2012. Privacy in the Age of Mobility and Smart Devices in Smart Homes. In *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*. 819–826. https://doi.org/10.1109/SocialCom-PASSAT.2012.108

[5] Natã M Barbosa, Joon S Park, Yaxing Yao, and Yang Wang. 2019. "What if?" Predicting Individual Users' Smart Home Privacy Preferences and Their Changes. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019), 211–231. https://doi.org/10.2478/popets-2019-0066

[6] Florian Bemmann, Maximiliane Windl, Jonas Erbe, Sven Mayer, and Heinrich Hussmann. 2022. The Influence of Transparency and Control on the Willingness of Data Sharing in Adaptive Mobile Apps. *Proc. ACM Hum.-Comput. Interact.* 6, MHCI, Article 189 (sep 2022), 26 pages. https://doi.org/10.1145/3546724

[7] 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

[8] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. 2016. On privacy and security challenges in smart connected homes. In *2016 European Intelligence and Security Informatics Conference (EISIC, 16)*. IEEE, 172–175. https://doi.org/10.1109/EISIC.2016.044

[9] 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

[10] Yuxin Chen, Huiying Li, Shan-Yuan Teng, Steven Nagels, Zhijing Li, Pedro Lopes, Ben Y. Zhao, and Haitao Zheng. 2020. Wearable Microphone Jamming. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376304

[11] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. 2012. Investigating Receptiveness to Sensing and Inference in the Home Using Sensor Proxies. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (Pittsburgh, Pennsylvania) *(UbiComp '12)*. Association for Computing Machinery, New York, NY, USA, 61–70. https://doi.org/10.1145/2370216.2370226

[12] 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

[13] Sarah Delgado Rodriguez, Sarah Prange, and Florian Alt. 2021. Take Your Security and Privacy Into Your Own Hands! Why Security and Privacy Assistants Should be Tangible. In *Mensch und Computer 2021 - Workshopband*, Carolin Wienrich, Philipp Wintersberger, and Benjamin Weyers (Eds.). Gesellschaft für Informatik e.V., Bonn. https://doi.org/10.18420/muc2021-mci-ws09-393

[14] Youngwook Do, Jung Wook Park, Yuxi Wu, Avinandan Basu, Dingtian Zhang, Gregory D. Abowd, and Sauvik Das. 2022. Smart Webcam Cover: Exploring the Design of an Intelligent Webcam Cover to Improve Usability and Trust. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 5, 4, Article 154 (dec 2022), 21 pages. https://doi.org/10.1145/3494983

[15] Anthony Dunne and Fiona Raby. 2013. *Speculative everything: design, fiction, and social dreaming*. MIT press.

[16] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 64, 16 pages. https://doi.org/10.1145/3411764.3445148

[17] Susanne Friese. 2020. Inter-Coder Agreement Analysis. http://downloads.atlasti.com/docs/ICA_a8_mac_en.pdf Accessed: 2022-12-12.

[18] Nina Gerber, Paul Gerber, Hannah Drews, Elisa Kirchner, Noah Schlegel, Tim Schmidt, and Lena Scholz. 2018. FoxIT: Enhancing Mobile Users' Privacy Behavior by Increasing Knowledge and Awareness. In *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust* (Orlando, Florida, USA) *(STAST '17)*. Association for Computing Machinery, New York, NY, USA, 53–63. https://doi.org/10.1145/3167996.3167999

[19] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. 2018. 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)*. USENIX, Baltimore, MD, USA. https://doi.org/10.5445/IR/1000083578

[20] Hana Habib, Yixin Zou, Yaxing Yao, Alessandro Acquisti, Lorrie Cranor, Joel Reidenberg, Norman Sadeh, and Florian Schaub. 2021. Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 63, 25 pages. https://doi.org/10.1145/3411764.3445387

[21] Woodrow Hartzog. 2018. The case against idealising control. *Eur. Data Prot. L. Rev.* 4 (2018), 423.

[22] Corey Brian Jackson and Yang Wang. 2018. Addressing The Privacy Paradox through Personalized Privacy Notifications. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 2, Article 68 (jul 2018), 25 pages. https://doi.org/10.1145/3214271

[23] Yunhan Jack Jia, Qi Alfred Chen, Shiqi Wang, Amir Rahmati, Earlence Fernandes, Zhuoqing Morley Mao, Atul Prakash, and SJ Unviersity. 2017. ContexIoT: Towards providing contextual integrity to appified IoT platforms.. In *NDSS*, Vol. 2. San Diego, 2–2.

[24] Haojian Jin, Boyuan Guo, Rituparna Roychoudhury, Yaxing Yao, Swarun Kumar, Yuvraj Agarwal, and Jason I. Hong. 2022. 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* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 449, 19 pages. https://doi.org/10.1145/3491102.3517602

[25] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI '10)*. ACM, New York, NY, USA, 1573–1582. https://doi.org/10.1145/1753326.1753561

[26] Nari Kim, Juntae Kim, Bomin Kim, and Young-Woo Park. 2021. The Trial of Posit in Shared Offices: Controlling Disclosure Levels of Schedule Data for Privacy by Changing the Placement of a Personal Interactive Calendar. In *Designing Interactive Systems Conference 2021* (Virtual Event, USA) *(DIS '21)*. Association for Computing Machinery, New York, NY, USA, 149–159. https://doi.org/10.1145/3461778.3462073

[27] Jacob Leon Kröger, Otto Hans-Martin Lutz, and Stefan Ullrich. 2021. The myth of individual control: Mapping the limitations of privacy self-management. *Available at SSRN* (2021).

[28] Hyosun Kwon, Joel E Fischer, Martin Flintham, and James Colley. 2018. The connected shower: Studying intimate data in everyday life. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 4 (2018), 1–22.

[29] Evan Lafontaine, Aafaq Sabir, and Anupam Das. 2021. Understanding People's Attitude and Concerns towards Adopting IoT Devices. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems (CHI'21)*. Association for Computing Machinery, New York, NY, USA, Article 307, 10 pages. https://doi.org/10.1145/3411763.3451633

[30] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 102 (nov 2018), 31 pages. https://doi.org/10.1145/3274371

[31] 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

[32] Huichen Lin and Neil W. Bergmann. 2016. IoT Privacy and Security Challenges for Smart Home Environments. *Information* 7, 3 (2016). https://doi.org/10.3390/info7030044

[33] Michal Luria, Guy Hoffman, and Oren Zuckerman. 2017. Comparing Social Robot, Screen and Voice Interfaces for Smart-Home Control. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 580–628. https://doi.org/10.1145/3025453.3025786

[34] Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. 2018. "What Can't Data Be Used For?" Privacy Expectations about Smart TVs in the US. In *Proceedings of the 3rd European Workshop on Usable Security (EuroUSEC), London, UK*. https://doi.org/10.14722/eurousec.2018.23016

[35] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019). https://doi.org/10.2478/popets-2019-0068

[36] 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/doi:10.2478/popets-2020-0035

[37] 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

[38] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys That Listen: A Study of Parents, Children, and Internet-Connected Toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 5197–5207. https://doi.org/10.1145/3025453.3025735

[39] Vikram Mehta. 2019. Tangible Interactions for Privacy Management. In *Proceedings of the Thirteenth International Conference on Tangible, Embedded, and Embodied Interaction* (Tempe, Arizona, USA) *(TEI '19)*. Association for Computing Machinery, New York, NY, USA, 723–726. https://doi.org/10.1145/3294109.3302934

[40] Vikram Mehta, Daniel Gooch, Arosha Bandara, Blaine Price, and Bashar Nuseibeh. 2021. Privacy Care: A Tangible Interaction Framework for Privacy Management. *ACM Trans. Internet Technol.* 21, 1, Article 25 (feb 2021), 32 pages. https://doi.org/10.1145/3430506

[41] Jaron Mink, Amanda Rose Yuile, Uma Pal, Adam J Aviv, and Adam Bates. 2022. Users Can Deduce Sensitive Locations Protected by Privacy Zones on Fitness Tracking Apps. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 448, 21 pages. https://doi.org/10.1145/3491102.3502136

[42] Andrés Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, and David Irwin. 2010. Private Memoirs of a Smart Meter. In *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building* (Zurich, Switzerland) *(BuildSys '10)*. Association for Computing Machinery, New York, NY, USA, 61–66. https://doi.org/10.1145/1878431.1878446

[43] Simon Moncrieff, Svetha Venkatesh, and Geoff West. 2007. Dynamic Privacy in a Smart House Environment. In *2007 IEEE International Conference on Multimedia and Expo*. 2034–2037. https://doi.org/10.1109/ICME.2007.4285080

[44] Mainack Mondal, Günce Su Yilmaz, Noah Hirsch, Mohammad Taha Khan, Michael Tang, Christopher Tran, Chris Kanich, Blase Ur, and Elena Zheleva. 2019. Moving Beyond Set-It-And-Forget-It Privacy Settings on Social Media. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (London, United Kingdom) *(CCS '19)*. Association for Computing Machinery, New York, NY, USA, 991–1008. https://doi.org/10.1145/3319535.3354202

[45] 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

[46] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Washington Law Review* 79 (2004), 119–158.

[47] Johannes Obermaier and Martin Hutle. 2016. Analyzing the Security and Privacy of Cloud-Based Video Surveillance Systems. In *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security* (Xi'an, China) *(IoTPTS '16)*. Association for Computing Machinery, New York, NY, USA, 22–28. https://doi.org/10.1145/2899007.2899008

[48] Robert W. Reeder, Patrick Gage Kelley, Aleecia M. McDonald, and Lorrie Faith Cranor. 2008. A User Study of the Expandable Grid Applied to P3P Privacy Policy Visualization. In *Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society* (Alexandria, Virginia, USA) *(WPES '08)*. Association for Computing Machinery, New York, NY, USA, 45–54. https://doi.org/10.1145/1456403.1456413

[49] Sarah Delgado Rodriguez, Sarah Prange, Christina Vergara Ossenberg, Markus Henkel, Florian Alt, and Karola Marky. 2022. PriKey – Investigating Tangible Privacy Control for Smart Home Inhabitants and Visitors . In *Proceedings of the 12th Nordic Conference on Human-Computer Interaction:* (Denmark) *(NordiCHI '22)*. Association for Computing Machinery, New York, NY, USA. http://www.florian-alt.org/unibw/wp-content/publications/delgado2022nordichi.pdf delgado2022nordichi.

[50] Tanuja Singh and Mark E Hill. 2003. Consumer privacy and the Internet in Europe: a view from Germany. *Journal of consumer marketing* (2003).

[51] Stephen Snow, Awais Hameed Khan, Mashhuda Glencross, and Neil Horrocks. 2021. Neighbourhood Wattch: Using Speculative Design to Explore Values Around Curtailment and Consent in Household Energy Interactions. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 643, 12 pages. https://doi.org/10.1145/3411764.3445095

[52] Eleftherios Spyromitros-Xioufis, Symeon Papadopoulos, Adrian Popescu, and Yiannis Kompatsiaris. 2016. Personalized Privacy-Aware Image Classification. In *Proceedings of the 2016 ACM on International Conference on Multimedia Retrieval* (New York, New York, USA) *(ICMR '16)*. Association for Computing Machinery, New York, NY, USA, 71–78. https://doi.org/10.1145/2911996.2912018

[53] Christian Tiefenau, Maximilian Häring, Eva Gerlitz, and Emanuel von Zezschwitz. 2019. Making Privacy Graspable: Can we Nudge Users to use Privacy Enhancing Techniques? https://doi.org/10.48550/ARXIV.1911.07701

[54] Yang Wang. 2018. Inclusive security and privacy. *IEEE Security & Privacy* 16, 4 (2018), 82–87.

[55] Maximiliane Windl, Niels Henze, Albrecht Schmidt, and Sebastian S. Feger. 2022. Automating Contextual Privacy Policies: Design and Evaluation of a Production Tool for Digital Consumer Privacy Awareness. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 34, 18 pages. https://doi.org/10.1145/3491102.3517688

[56] 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 (nov 2022), 20 pages. https://doi.org/10.1145/3567739

[57] 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

[58] Xiaokui Xiao and Yufei Tao. 2006. Personalized Privacy Preservation. In *Proceedings of the 2006 ACM SIGMOD International Conference on Management of Data* (Chicago, IL, USA) *(SIGMOD '06)*. Association for Computing Machinery, New York, NY, USA, 229–240. https://doi.org/10.1145/1142473.1142500

[59] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. 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/10.1145/3290605.3300428

[60] 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

[61] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 200 (nov 2018), 20 pages. https://doi.org/10.1145/3274469