PrivacyHub: A Functional Tangible and Digital Ecosystem for Interoperable Smart Home Privacy Awareness and Control

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

Philipp Thalhammer
LMU Munich
Munich, Germany
philipp.thalhammer@ifi.lmu.de

David Müller
LMU Munich
Munich, Germany
david.muelle2@web.de

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

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

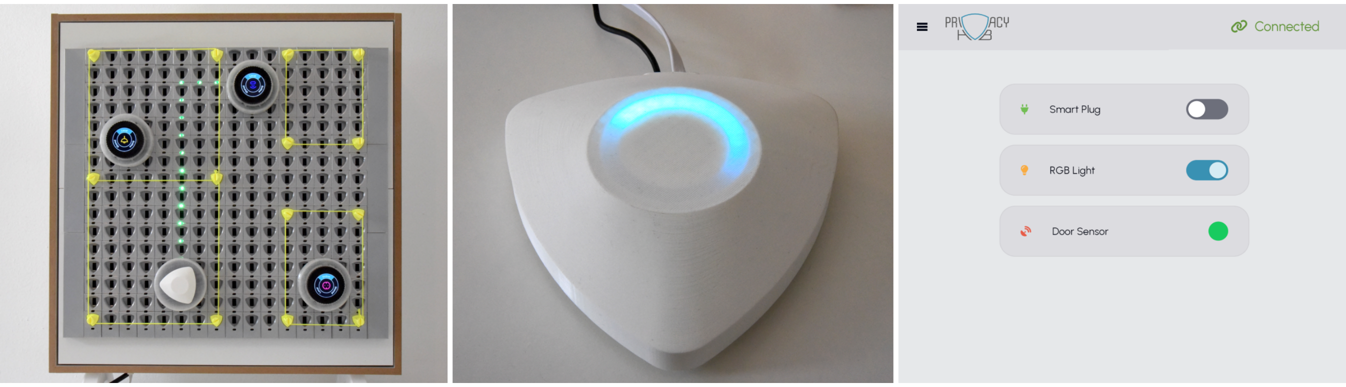


Figure 1: Left is the physical dashboard with yellow strings visualizing the floor plan and proxies representing the smart devices. Users can adjust privacy states by turning the proxy's ring; LEDs then indicate data streams. The top-right is the privacy hub, the system's communication unit, and the bottom-right is the web application for digital control.

Abstract

Hubs are at the core of most smart homes. Modern cross-ecosystem protocols and standards enable smart home hubs to achieve interoperability across devices, offering the unique opportunity to integrate universally available smart home privacy awareness and control features. To date, such privacy features mainly focus on individual products or prototypical research artifacts. We developed a cross-ecosystem hub featuring a tangible dashboard and a digital web application to deepen our understanding of how smart home users interact with functional privacy features. The ecosystem allows users to control the connectivity states of their devices and raises awareness by visualizing device positions, states, and data flows. We deployed the ecosystem in six households for one week and found that it increased participants' perceived control, awareness, and understanding of smart home privacy. We further found distinct differences between tangible and digital mechanisms. Our findings highlight the value of cross-ecosystem hubs for effective privacy management.

CCS Concepts

• **Security and privacy** → *Usability in security and privacy*; • **Human-centered computing** → **Human computer interaction (HCI)**.

Keywords

human-computer interaction, smart home privacy, tangible privacy, smart home dashboard, privacy awareness, privacy control

CHI '25, Yokohama, Japan
© 2025 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 979-8-4007-1394-1/25/04
https://doi.org/10.1145/3706598.3713517

ACM Reference Format:
Maximiliane Windl, Philipp Thalhammer, David Müller, Albrecht Schmidt, and Sebastian S. Feger. 2025. PrivacyHub: A Functional Tangible and Digital Ecosystem for Interoperable Smart Home Privacy Awareness and Control. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3706598.3713517

1 Introduction

Smart home devices offer various benefits, such as increased comfort through the automation of monotonous tasks, increased safety and security through smart health monitors and security systems, or better energy efficiency through smart lights and smart thermostats. The devices have various sensors and capabilities that constantly collect and process personal user data to enable these functionalities. Yet, this also paves the way for security and privacy risks as the data can get abused to infer and disseminate sensitive user data, such as identities and behavior [5, 38, 40]. While many users lack knowledge and awareness of the privacy-relevant processes and vulnerabilities of smart home devices [21, 32, 33], many still express concerns about the nefarious use of their data and try to address their privacy concerns by engaging in privacy-protective behaviors, such as unplugging devices [26]. However, such drastic measures that disable all functionality at once are often excessive, as concerns mostly refer to specific sensors or capabilities.

To support users in their desire for granular control, some smart home manufacturers integrate privacy features into their products, such as physical camera shutters or mute buttons. This is in line with prior research developing a range of prototypical research artifacts, such as automatic [16] and manual [50] camera shutters, a prototype in the shape of a key that allows disabling all sensors of a specific type [15], or a prototype that allows adjusting the network connectivity of smart devices [17]. Yet, all these efforts lack interoperability, i.e., they only work for specific, individual devices, address only a subset of sensors, or have remained in their prototypical state. Thus, we currently do not know how users interact with functional, universal privacy features on a day-to-day basis. Smart home hubs, serving as the central control units within a smart home, provide an ideal foundation for a centralized privacy management system. However, it is only recently that universal standards, such as the Matter standard[1], have enabled seamless, cross-device access and control. Additionally, no commercially available hubs offer tangible cross-platform privacy features or provide device users and bystanders with a clear understanding of nearby devices, their connection status, or data flows.

We leveraged these recent advancements and developed a fully functional smart home ecosystem consisting of a cross-ecosystem hub, a tangible dashboard, and a web application that provides privacy awareness and control to smart home users. We decided to incorporate tangible features as prior work frequently emphasized their advantage for smart home privacy and control, highlighting values such as high trust and understandability [3, 50], which ultimately contribute to inclusive privacy for all stakeholders in a smart home. Concretely, the ecosystem consists of a tangible dashboard that builds on validated concepts from prior work by indicating the smart devices' locations [48, 50] and privacy states [17] with device proxies. The dashboard allows tangible control over the devices' network connectivity states and provides awareness by visualizing data flows. In detail, and in line with current research efforts [17, 43], the digital application and physical dashboard allow users to adjust the privacy states of individual devices to only be accessible within the network, from the outside via a secure gateway or through a third-party hub. Whenever a privacy state is changed, the dashboard visualizes the data flows using LED stripes to raise the user's privacy awareness. We deployed the smart home ecosystem in six households with 13 participants for one week to investigate how smart home users interact with it and how it changes their privacy awareness, knowledge, and behavior. For that, we logged participants' interactions with the ecosystem's digital and physical components, asked users to fill out questionnaires before and after the study, and conducted a concluding interview. We found that all participants appreciated the ecosystem as a control and privacy hub. Our findings indicate that participants generally agreed that interacting with the system heightened their awareness of privacy risks, led to more privacy-conscious decisions, and enhanced their understanding of privacy-relevant processes through the visualization of data streams. Additionally, participants expressed a slight overall preference for adjusting privacy settings via haptic interaction, though this preference varied by household. Participants also emphasized the distinct advantages of tangibility, such as immediate feedback, increased trust, and continuous reflection, reinforcing the case for tangible privacy mechanisms.

This work contributes to privacy research by strengthening the importance of providing privacy mechanisms and emphasizing the value of tangible interactions through lived experiences with a functional cross-device privacy hub. Based on our findings, we recommend that researchers and product designers systematically explore interoperability concepts in smart homes as drivers for more accessible privacy awareness and control mechanisms. We further contribute our system's code and all 3D models to enable practitioners and researchers to build upon and extend our system: https://github.com/mimuc/PrivacyHub.

2 Related Work

We start by reviewing prior work on privacy risks and mitigation strategies in smart homes, highlighting the roles of different user groups and their unique challenges, before summarizing research on tangible privacy mechanisms.

2.1 Smart Home Privacy Risks, Concerns, and Strategies

Smart home devices have the potential to reveal especially sensitive data as they are placed in our most intimate spaces. Research already showed how data collected in homes can be exploited to reveal identities [40] and user's behavioral patterns, such as when they leave their homes or sleep [5, 38]. Hence, many users express concerns about smart home devices, such as being exposed to always-listening smart speakers that might reveal sensitive data without explicit consent, targeted advertising, or data getting shared with third parties [29, 30]. Privacy concerns are also influenced by the device's sensors. Prior research, for example, showed that users are exceptionally concerned about microphones and cameras [11, 49],

[1] https://csa-iot.org/all-solutions/matter

whereas they do not consider temperature or motion sensors nearly as concerning [10, 39, 49, 56]. Also, the social relationship with the device owner has an impact on privacy concerns. A study by Yao et al. [53] suggests that people are more accepting of devices that belong to a trusted person. Yet, greater familiarity can also increase data sensitivity as people with a great knowledge of a person can make sense of personal data more easily [25, 51].

When discussing desired data protection strategies, Yao et al. [52] found that users frequently suggested keeping data local rather than sending it to remote servers and disconnecting devices from the internet while retaining offline functionality. Similarly, Jin et al. [26] found that many users unplug their devices to protect their privacy. When asked about preferred data-protection features, most users favored automated or remote controls to turn devices off, four requested more granular control over data collection, and one advocated for local-only network communication. To address these user preferences, Feger et al. [17] introduced a framework enabling device functionality across four connectivity modes: online, local network, access point mode, and offline. They demonstrated this approach using a prototype smart camera and an environmental sensing unit. Building on this concept, Thalhammer et al. [43] added awareness features by visualizing changes in information flow based on connectivity mode adjustments.

2.2 Multi-User Privacy in Smart Homes

Often, multiple people live in one household, but only one person is responsible for managing smart devices, which can lead to knowledge gaps and power imbalances [19, 31, 55]. Research divides these user groups into primary and secondary users [2, 30] or pilot and passenger users [28], whereby the secondary (or passenger) user interacts with the devices but does not have full control [2, 30]. Secondary users often have no options to protect themselves against monitoring by the primary users [2], and in extreme cases, smart home devices can even be abused to spy on partners [31].

Another important user group is incidental users [30] or bystanders, i.e., people who are not the primary users of a device but are nevertheless exposed to it [49], such as temporary guests. Research emphasizes that this user group is especially protection-worthy as they can often not choose to be exposed to the devices or lack the right tools to express preferences or exert control [30, 34–36]. Yao et al. [53] found that bystanders were most concerned about data captured by microphones and videos and mitigated their concerns by covering cameras or placing devices in less sensitive rooms. In the context of Airbnb rentals, Mare et al. [34] found that guests were most concerned about hosts spying on them or being discriminated against based on their behavior. Alshehri et al. [4] found that many smart device owners don't inform bystanders about privacy practices because they don't fully understand them. While 35% of owners agreed that *"visitors have no privacy rights in my smart home,"* 45% disagreed, and 25% saw privacy disclosure as unnecessary. In contrast, 72% of bystanders felt uncomfortable with their data being collected by others' devices. This highlights the dilemma of informing bystanders, as owners may not feel obligated or fully grasp the privacy implications themselves.

Table 1: Comparison of PrivacyHub with related systems.

	SaferHome [48]	**PriKey [15]**	**Dashboard [50]**	**PrivacyHub**
Focus	Primarily Security	Privacy	Privacy	Privacy
Purpose	Visualizes device vulnerabilities	Simulates sensor disabling	Visualizes device capabilities and locations	Enables cross-platform tangible privacy control and awareness
Status	Functional, connected prototype	Wizard-of-Oz prototype	Non-functional (wooden mockup)	Fully functional, cross-platform prototype
Awareness vs. Control	Awareness only	Primarily control	Awareness only	Combines awareness and control
Goal	Raise awareness of security vulnerabilities	Enable quick deactivation of sensors	Increase awareness of device capabilities	Provide integrated privacy control and awareness across platforms

2.3 Tangible Privacy Mechanisms

Tangible privacy mechanisms have been suggested by prior research to provide awareness and control in smart homes, as they instill high trust in users and are easily understandable independent of technological understanding [3, 14, 37], which contributes to inclusive privacy [50]. Ahmad et al. [3] were the first to introduce the concept of "tangible privacy" and argue that sensors should have physical control mechanisms and provide unambiguous feedback on what data is currently collected. Delgado Rodriguez et al. [13] further found that tangible mechanisms positively impacted users' awareness of risks and ease of verification, and participants in a study of Chalhoub et al. [11] desired tangible mechanisms, especially in sensitive locations, such as a smart display placed in a bathroom. Once the participant placed the shutter in front of the camera, they were comfortable placing the device in the bathroom.

Concrete prototypes of tangible privacy mechanisms include a wearable microphone jammer to disable microphones in the user's vicinity [12], a cover to disable smart speakers' microphones [44], a calendar that only reveals private appointments when placed in private locations [27], a smart webcam cover that automatically blocks the camera when it is not in use [16], and a key that allows users to deactivate all sensors of a specific type for individual rooms [15]. Another example is tangible smart home dashboards that visualize the devices' locations within the user's floor plan and provide either warnings about security vulnerabilities and updates [48] or information about the devices' capabilities [50]. Both studies found that the boards were effective in raising users' privacy awareness, and Windl et al. [50] argue that future smart home dashboards should provide awareness and control instead of focusing on a single dimension. Prior work further demanded that tangible control artifacts should be *"bundled in a central control unit"* [50]. Table 1 summarizes the key differences between PrivacyHub and related systems that were suggested by prior work.

2.4 Summary and Research Questions

Prior work has shown that users are concerned about their data privacy in smart homes [29, 30, 49]. Yet, privacy risks and concerns affect not only primary users but also multiple stakeholders in smart homes, including secondary users and bystanders. These users are especially protection-worthy as they often lack sufficient knowledge to protect their private data [2, 31, 36]. To tackle their concerns, users, as well as bystanders in smart homes, wish for control options [52, 53]. Yet, since smart home devices currently only offer limited privacy control, they often have to resort to taking their devices off the internet or unplugging them, which disables all functionality and renders the smart device useless [11, 26]. In an effort to enable more granular control and keep device functionality, prior work envisioned a control framework for the device's internet connectivity [17]. As tangible privacy mechanisms are intuitive and increase trust [3], tangible smart home dashboards have been suggested to provide privacy awareness for owners and bystanders [48, 50]. Prior research further demanded that tangible control mechanisms should be integrated into a central control unit [50]. We bring together these research threads to create a cross-device smart home privacy ecosystem that integrates tangible and digital mechanisms to improve privacy control and awareness. We examine its impact on privacy awareness, understanding, and interactions through the following research questions:

RQ1 How do users perceive the focus on privacy in the interaction with a cross-ecosystem smart home hub?

RQ2 How are tangible and digital privacy features used in highly interoperable smart home systems?

3 System

We developed a functional cross-platform smart home ecosystem to enhance users' privacy awareness and control. The system includes a smart home hub and a web interface, enabling users to connect devices, adjust connectivity states digitally, and use a history feature to track when devices were active and their respective connectivity states. Additionally, the ecosystem incorporates a tangible dashboard that (1) provides privacy control by allowing users to change device connectivity states and (2) increases privacy awareness by visualizing data flows within the smart home. As a proof of concept, our system currently supports three device types: door sensors to detect open doors, smart lights, and smart power plugs, with the on/off functionality of the smart lights also implemented using a smart plug. The selection of devices was limited to those that (a) support the Matter standard and (b) use the Thread protocol for communication, which we anticipate will become common across most devices in the coming years. The Matter standard addresses the heterogeneity of smart homes by providing a unified communication protocol across various IoT devices, regardless of manufacturer or underlying technology [54]. It ensures interoperability and serves as the application layer in PrivacyHub, enabling seamless device communication[2]. Thread, an IoT protocol released in 2015 [45], provides a secure, low-power communication network within a Private Area Network (PAN) and is widely adopted in smart home devices. In PrivacyHub, Thread facilitates device-to-device and device-to-hub communication, while Matter ensures interoperability across devices from different manufacturers. Together, these protocols enable PrivacyHub to function as an interoperable smart home hub. The system also allows connecting to third-party hubs like Amazon Alexa, Google Smart Home, or Apple HomeKit to enable additional features such as voice control. In the following, we explain all system components in detail. We open-source all code and 3D models to allow future research to build on our system: https://github.com/mimuc/PrivacyHub.

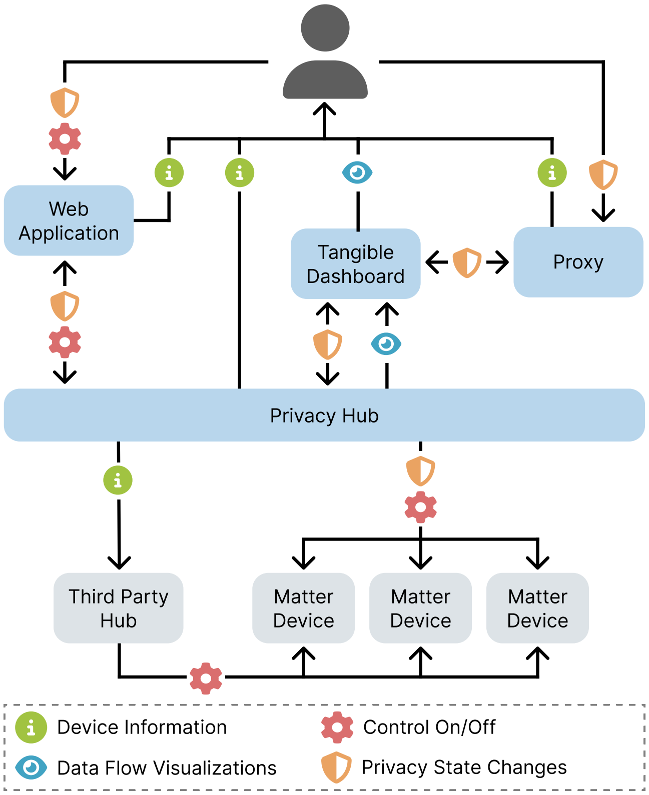


Figure 2: Overview of the communication architecture. The privacy hub mediates communication between users, smart home devices, and third-party hubs: The proxies facilitate privacy state changes and device control; the tangible dashboard provides awareness through the data flow visualizations; and the web application allows remote access and control.

3.1 Concept

In line with the concepts from prior work [17, 43], we allow users to adjust the device connectivity to three states:

(1) **Local Mode.** This mode restricts the device's access to the same network. While it is the most secure state, it also has the least features.
(2) **Online Mode.** This mode allows device access via the online front end, meaning the user can access it from anywhere with an internet connection. Since the data is leaving the home network, this state offers less privacy as it opens potential attack vectors. Yet, the system is still in control over where the data is going.
(3) **Online-Shared Mode.** This mode allows pairing with a third-party hub like Amazon Alexa. While this state offers more features like voice control and automation, the system can no longer guarantee the integrity of the data, as it can now be accessed by a third-party device.

[2] https://csa-iot.org/all-solutions/matter

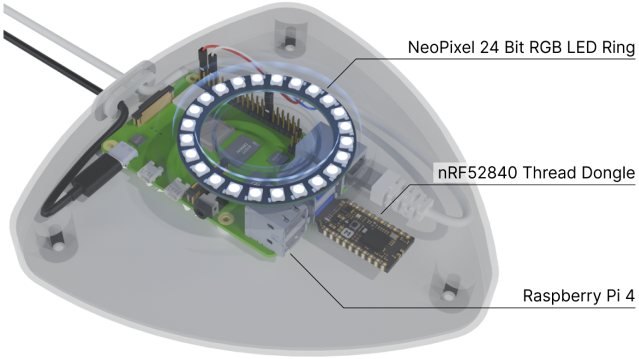


Figure 3: Internal components of the smart home privacy hub. The hub features a NeoPixel 24-bit RGB LED ring for visual feedback, an nRF52840 thread dongle enabling wireless communication via the Thread protocol, and a Raspberry Pi 4 serving as the primary processing unit.

The dashboard maps a household's floor plan on which users can place proxies that represent smart home devices and the smart home hub. Users can directly adjust the device connectivity by turning the ring on these proxies. They also display the device's current state on a small display. The dashboard automatically detects the position of the plugged-in proxies and communicates with the hub to visualize the real-time data flow between the devices using integrated LEDs. The LEDs can display three different animations: (1) a plug-in animation that lets the LEDs adjacent to a coordinate pulse six times, (2) a path between two coordinates that gets repeated six times to visualize data flows, and (3) a start-up animation that signals that the system has finished booting. The data flow animations always happen between the proxies and the hub. The data can either flow from a proxy to the hub in case the user changes the privacy state on the tangible dashboard or from the hub to the proxy when the user changes the privacy state or controls a device via the front end. We created three device proxies for our prototype to test in the user study. However, the dashboard's design allows for accommodating as many proxies as its size permits. Figure 2 shows the system's communication architecture.

3.2 Smart Home Hub

The smart home hub is the central control unit of the ecosystem and consists of a physical hub and an accompanying web application. It can support current commercial products that implement the Matter standard and consists of a 3D-printed case that holds a Raspberry Pi 4, see Figure 3. For better performance, we plugged a BLE dongle into the Pi and equipped a second USB port with an nRF52840 Thread Dongle to enable Thread communication. The hub has an LED Ring near the top of the upper case to give users visual feedback on the system status. It flashes white when starting up and turns to blue when it is on. It further flashes once in the respective color when the privacy state of one of its connected smart home devices is changed: Red for online-shared, orange for online, and green for local.

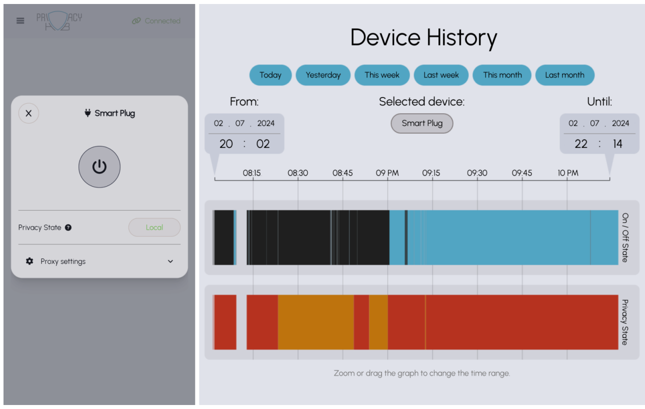


Figure 4: The web interface. The left part shows controls for a smart plug, enabling users to toggle devices on or off and modify privacy states. The right part shows the device history. Black and blue represent the on/off state of the device, while orange and red indicate different privacy states. Black means off, blue on, orange online, red online-shared.

The user can also interact with the system using the responsive web application, which has a local and remote front end. When a device is set to local mode, it can only be controlled from the local front end, requiring the user to be in the same network as the smart home hub. In contrast, the remote front end requires devices to be set to online or online-shared mode and allows users to control them from anywhere. Developing a responsive web app reflects industry standards, as many native apps use frameworks like React. This ensured compatibility across devices, allowing participants to use their own devices for natural interactions and reducing technological overhead, see Figure 4 (left). To use the app's remote version, users need to log in. After pairing a device, the user is directed to the digital dashboard, which provides an overview of all available devices. The user can click on a device to receive additional information and adjust the privacy states. The history subpage allows users to review past device states. The user can use the buttons at the top or enter dates to choose a time range. The gap visualized in Figure 4 (right) indicates that the device was in local mode shortly before 8:15, as the online front end does not have access to data when devices are set to local.

3.3 Dashboard

The tangible dashboard measures 20 inches × 20.5 inches × 4 inches. It consists of 16 custom-made printed circuit boards (PCBs) with a grid of four-by-four DuPont plugs. The PCBs (i.e., tiles) are arranged in a four-by-four grid and daisy-chained together, resulting in 256 plugs. The first tile is injected with 5 Volts (V) at 3 Amperes (A), which gets transferred to the rest of the tiles. Figure 5 shows a cross-section of the dashboard. The tiles are positioned between a piece of wood and two plastic sheets, with small silicon bumpers on both sides to protect the resistors. Spacers on all four sides of the dashboard hold the tiles in place. We placed high-resolution LED strips on the plastic sheets to visualize the data streams. To make connecting and aligning the proxies easier, we 3D printed small

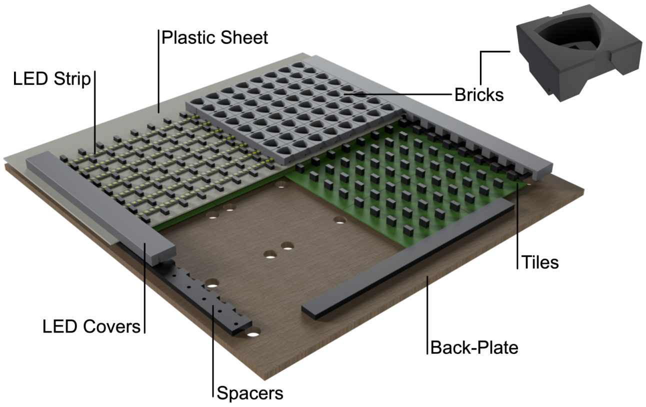


Figure 5: A cross-section of the tangible privacy dashboard. The dashboard features a back plate for structural support and LED strips for visual feedback. A plastic sheet secures the components, and spacers hold the tiles in place.

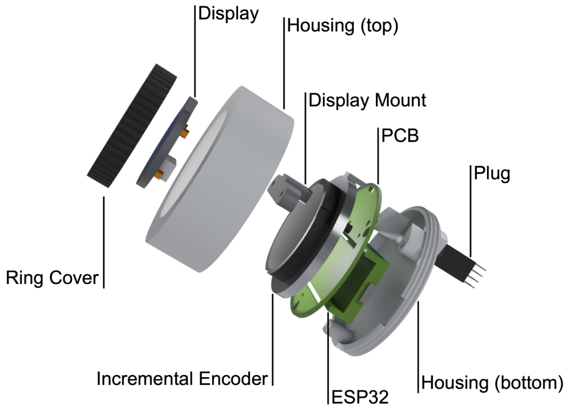


Figure 6: An exploded view of a proxy with its key components: The ring cover, incremental encoder, display, PCB, ESP32 microcontroller, and plug, all enclosed within the top and bottom housing.

bricks with a key-lock system, see Figure 5. We glued the bricks to the plastic sheets and enclosed the dashboard in a wooden frame to hide the electronic components. We also 3D-printed poles to hold a string that serves as the visualization of the floor plans.

Each plug features eight connectors. GND and 5V are used to power the plugged-in proxy. ROW and COL have different voltages depending on their position on a tile: The ROW-pin voltage decreases from 5V at the top to 0V at the bottom in four steps, and the COL-pin voltage decreases the same way from left to right. The proxy uses these two pins to determine the relative position on the board. The TILE-pin is used to get information about the tile to which the proxy is connected. The TILE-pin voltage decreases from 5V to 0V in 16 steps, each step representing one of the 16 tiles. By combining the relative position from the ROW and COL-pin with the information from the TILE-pin, it is possible to calculate the absolute position of a proxy on the dashboard. The code for the dashboard runs on a Raspberry Pi 4B, and the communication between the dashboard and the proxies is handled with MQTT. The Raspberry Pi is connected to the internet via LAN and hosts an access point for the proxies to reduce the dashboard's set-up effort. The LEDs are controlled by an ESP32 microcontroller, which receives messages from the Raspberry Pi via USB serial.

3.4 Proxies

The proxies represent the smart home devices and the smart home hub on the dashboard and enable users to change the connectivity states. Figure 6 shows a cross-section of the proxies. Each proxy has a 3D-printed housing screwed together to allow easy access to the microcontroller. The display is connected to a PCB via a wired connection with a detachable socket and screwed to a 3D-printed mount, which is then screwed onto the PCB. The incremental encoder, which is used to change the device's connectivity state, is also screwed and soldered to the PCB. See Figure 7 for a picture of the proxy display. The plug has seven cables, which are soldered to the PCB, placed into an eight-pin DuPont plug, and glued into the bottom part of the housing. Finally, the PCB gets mounted onto three designated stilts on the bottom part of the housing. A 3D-printed ring cover can then be pressure-fitted over the incremental encoder to provide a better grip and cover the wiring.

As the ESP32 operates at 3V, but the position information gets represented in a range of 5V to 0V, we use voltage dividers to reduce the incoming voltages. When booting, the proxy first reads the three voltages for the position calculation. After this, the proxy connects to the dashboard access point and establishes a connection to the MQTT broker. It then publishes the three voltage readings and continues to listen for changes in the position of the incremental encoder as well as state updates from the hub. If a change is detected, the UI gets adapted to display the correct state. The UI displays an icon in the center representing the corresponding device and highlights its current connectivity status in blue (see Figure 7).

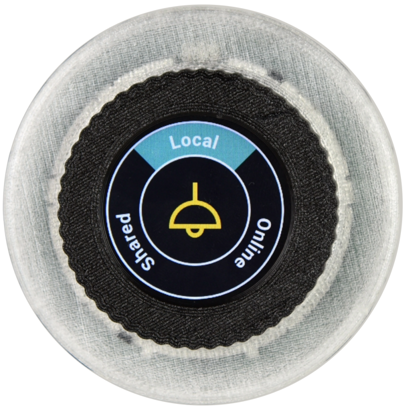


Figure 7: A close-up of a proxy interface with the three privacy states: Local, Online, and Online-Shared. Users can switch between privacy states by turning the black ring.

4 Method

We deployed PrivacyHub in six households, each for a week, to explore how users perceive privacy in interactions with a cross-ecosystem smart hub (**RQ1**) and examine how they engage with tangible and digital privacy features (**RQ2**).

4.1 Procedure

We gave participants a brief introduction and asked them to sign a consent form while we set up the system. This involved connecting the LAN and power for the dashboard and hub, as well as pairing a smart socket, a smart door sensor, a smart light, and an Alexa smart speaker. The participants could freely choose where they wanted to place the devices. We only required the dashboard to be placed at a location where it is clearly visible. After the initial setup, we explained the concept and core functionality of the system, including the three privacy states and the functionality of the tangible dashboard. We then asked participants to fill out a questionnaire about demographic data and other questions regarding their experience and behavior with smart home devices. Next, since participants were not required to have technical expertise, we conducted a detailed show-and-tell session to explain how the system worked. This included the use of the web application, the hub's functionality, and interacting with the dashboard by plugging in proxies, changing their privacy settings, and creating a floor plan. The participants were also instructed on how to handle minor errors in case the system stopped working, which mostly consisted of restarting different components. The participants were instructed to use the system as they saw fit but should interact with it at least once per day. After one week, we asked participants to complete another questionnaire about their experience with the system, followed by an interview where we discussed their experiences.

4.2 Measurements

All participants, except one, were German speakers, so most interviews and questionnaires were conducted in German. The English versions of all statements and questions are provided in Appendix Section A.1. In the first section, we gathered demographic information, including the number of smart devices participants had installed in their homes. Moreover, we asked participants to self-identify as pilot or passenger users ($\mathbf{Q_U}$**1**) according to [28]. We used the ATI scale [18] to assess participants' affinity for technology. We formulated $\mathbf{Q_S}$**1-8** to survey participants' (1) experience with smart home devices, (2) generally perceived importance of privacy, (3) importance of the smart device's features, (4) importance of the smart device's privacy protection, (5) control over privacy in their smart home, (6) concern about their privacy in their smart home, (7) knowledge about how to protect privacy in their smart homes, and (8) knowledge about data practices in their smart home. Finally, in $\mathbf{Q_S}$**9**, we asked how frequently participants interact with smart home devices with the following options: '*multiple times per day*,' '*once per day*,' '*multiple times per week*,' '*once per week*,' '*multiple times per month*', and '*never*.' After one week, we asked participants to fill out a second questionnaire featuring $\mathbf{Q_S}$**1-8** and the *SUS* questionnaire [8] for both the hub and the dashboard separately. We also conducted a semi-structured interview, where we asked about participants' general experience with the system and specific questions about the privacy hub and the tangible dashboard. See $\mathbf{Q_I}$**1-23** for all interview questions. In addition, we recorded all interactions with the system, including device control and privacy state changes – both on the tangible dashboard and in the web application.

4.3 Participants

We recruited six households with thirteen participants (six male and seven female) via convenience sampling. They were between 25 and 54 (M = 29.77, SD = 10.34) years old. Five participants self-identified as pilot users, and eight as passenger users. The participants who self-identified as pilot users had a mean affinity for technology according to the ATI scale [18] of 5.2 (SD = .66), and the passenger users had a mean ATI score of 3.83 (SD = 1.04). All participant details are listed in Table 2. Most participants (P1, P2, P4, P5, P7, P8, P9) reported using smart home devices multiple times per day, three participants (P6, P10, P11) used them multiple times per week, and one participant (P3) used them once per day. The configured dashboard for each household can be seen in Figure 8. We could not install the smart lights in household H1 due to technical difficulties. We compensated all participants with 25€.

4.4 Data Analysis

We conducted thematic analysis [7] of our qualitative data and transcribed the interviews using Whisper[3], followed by manual corrections to address errors. We then used Atlas.ti to code our data. For that, two researchers independently coded an interview, met to discuss their codes and resolve disagreements, and formed a joint codebook. Three researchers then coded the rest of the interviews. After that, they met to form code groups and themes through multiple rounds of discussions. This process led to 218 codes, 17 code groups, and 3 overarching themes. We translated all direct quotes into English. We used Python to analyze our quantitative data.

[3] https://openai.com/index/whisper/

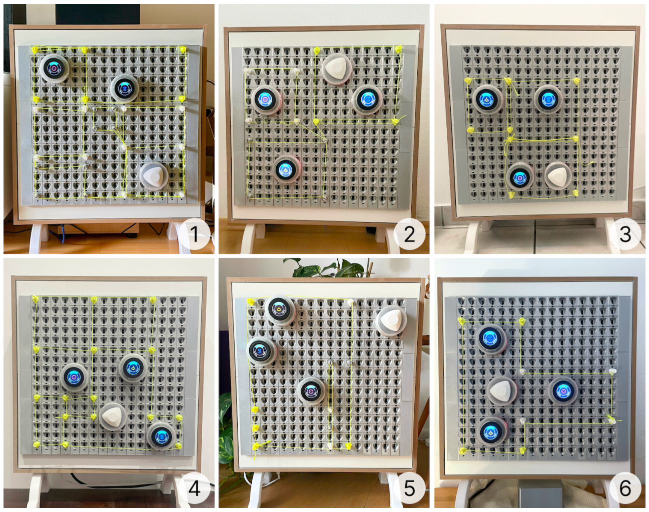


Figure 8: The configured dashboards displaying participants' floor plans and device placements.

Table 2: Household information and participant details, including their number of smart home devices (#), participant ID (PID), role, age, gender, profession, highest level of education, and technical affinity.

HID	#	PID	Role	Age	Gender	Profession	Education	ATI
H1	20	P1	Pilot	53	M	Banker	Vocational Training	5.22
		P2	Passenger	54	F	Housewife	Vocational Training	2.33
H2	1	P3	Passenger	25	F	Scientific Assistant	Bachelor	3.78
		P4	Pilot	26	M	Student	Vocational Training	4.33
H3	8	P5	Pilot	26	M	Editorial Journalist	Bachelor	4.78
		P6	Passenger	20	F	Student	High School	2.89
H4	16	P7	Passenger	26	M	IT Consultant	Master	5
		P8	Pilot	25	M	Consultant	Master	5.78
		P9	Passenger	24	F	Student	High School	5.11
H5	3	P10	Pilot	29	M	Electrical Engineer	Master	5.89
		P11	Passenger	29	F	IT Consultant	Master	4.22
H6	3	P12	Passenger	25	F	Student	Bachelor	2.89
		P13	Passenger	25	F	Student	Bachelor	4.44

4.5 Method Reflexivity

Our research investigates how increasingly interoperable smart home systems influence the applicability and use of privacy features. To explore this, we developed PrivacyHub, a smart home hub that enables users to interact with a variety of connected devices from different manufacturers, provided they utilize widely adopted standards and protocols like Matter and Thread.

Surveying related work in smart home privacy, we found that researchers highlight the value of both digital and tangible artifacts for enhancing privacy awareness and control. To explore the suitability of privacy features for device-independent, interoperable smart home systems, we incorporated both digital and tangible privacy tools in our study. Importantly, these tools do not offer the same feature set—a deliberate choice that contrasts with research focused on directly comparing matched tangible and digital dashboards [48]. Our aim is not to empirically compare tangible and digital interactions for smart home privacy but to introduce a range of established and experimental tools across the tangible-digital spectrum. This approach allows us to study the real-world applicability of privacy features in future interoperable smart homes that integrate devices across different types, manufacturers, and ecosystems. To this end, we avoided replicating the tangible dashboard on the web application, instead designing a straightforward, responsive digital interface using standard UI components. This approach ensures our investigation balances familiar and experimental privacy tools to better understand their roles in an interoperable, privacy-first smart home hub.

5 Results

We conducted an in-depth qualitative analysis and an exploratory quantitative analysis. Given the sample size, the quantitative analysis primarily complements the qualitative findings.

5.1 Interview Findings

We present the thematic analysis results under three themes: *System Perception*, *System Interaction*, and *Physical vs. Digital.*

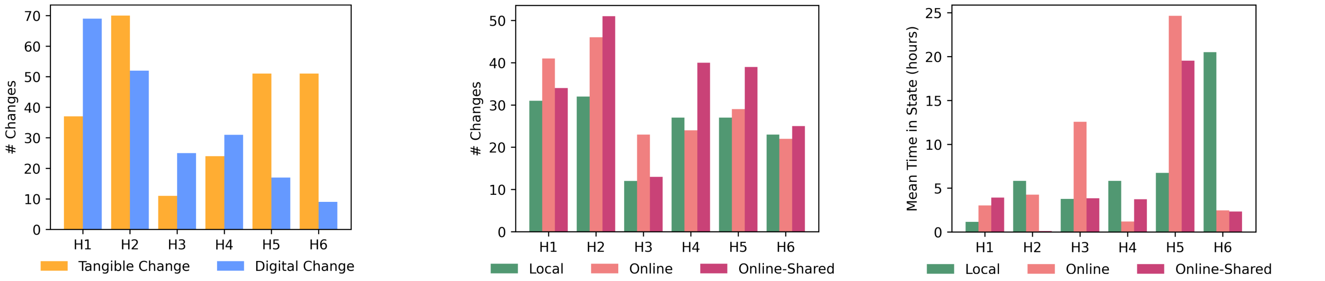
5.1.1 System Perception. This theme explores participants' perceptions of the system components, including their views on the data stream visualization and the floor plan representation. Participants agreed that the engagement with the system raised privacy awareness (P1, P3-P6, P8, P9). Especially the constant presence of the physical components in a prominent location, i.e., the hub and the dashboard, led to constant privacy reflections (P10, P11, P13): *"Every time we left the house, we saw the dashboard and knew right away, okay, how is it set right now? In that sense, it was just much more visible. And because you had to set it yourself, I think you just thought a lot more about how it should be set for the hours when you leave the house"* (P13). While some participants did not think that the system helped them make better privacy decisions (P5, P7, P9), others emphasized that the system definitely did (P11-P13): *"It helped me make better privacy decisions. Simply because I had to make decisions. Something that I hadn't considered at all before"* (P11). Some participants discussed that the system requires that users trust it to really protect their privacy as it claims to do (P1, P10, P13). Yet, in this regard, P10 stressed that the ecosystem was still the better choice as it reduces the complexity and, with that, the risk for privacy violations from multiple to only one device. Most participants liked the data stream visualizations (P1-P5, P7, P9, P10) and they discussed how they helped them understand the internal processes (P1, P4, P6, P12): *"Being able to see how devices communicate with each other also highlights, so to speak, data security a bit, because it gives me the feeling that data becomes visible"* (P4). Yet, P7 discussed how the constant flows might get annoying over time, especially if a user has a lot of smart devices that constantly trigger various data streams. In this regard, P11 suggested changing the behavior after an initial phase to only visualize unusual data streams, and P6 suggested only visualizing data streams that leave the internal network. In addition to the data streams, the privacy hub flashed in the respective color when a privacy state was changed. Yet, most participants stated that they had not noticed this visualization, and if so, they mainly considered it a visualization of the internal system status, i.e., signaling that the hub was connected and working (P1, P4, P10). Yet, P6 saw the visualization as a notification mechanism relevant in a co-inhabitant scenario: *"When you change something without the consent of others, it's definitely good to know that something has been altered because when you live with other people, it also concerns them."* Participants generally appreciated the floor plan representation (P1, P4, P7, P12), noting how it aided orientation and increased awareness of the number of smart devices in each room (P10). P12, who identified as non-technical, particularly valued the floor plan for its simplicity and clarity, finding it easier to understand than charts or tables.

5.1.2 System Interaction. This theme describes how participants used the system when they adjusted privacy states, why they did so, and how they integrated the system into their daily routines. For most participants, the PrivacyHub served as a control unit, i.e., to turn smart devices on and off (P3-P7, P9, P11, P13), as a privacy tool to switch between the privacy states (P1, P3-P5, P7, P8, P10, P12), and as a management tool to check the current state of their devices (P8, P10). Many participants changed between the privacy states when entering or leaving home (P10-P13), as P13 explains: *"Most of the time, when I came home or when I had just left the house, I always thought about whether I needed the device when I was out and about and if not, then I left it on local or when I came home and realized, okay, now I'm at home anyway, now I only need local, then I switched it to local."* P10 described how adjusting the privacy state became part of their routine when leaving the house, similar to grabbing their purse and keys. Hence, P10 also said that they would place the dashboard next to their entrance to support this workflow better. Two participants stated to only switch to the online-shared mode when they actively needed the feature, i.e., wanted to use voice control (P12, P13): *"I would just switch to shared when I wanted to use the feature. And then I would go right back to, like, localized"* (P12). When participants were outside their homes, they would log in to the web application to check the privacy state and state of their devices, for example, to check if they had locked their door or to heat up the coffee machine before they arrived back home (P8, P10-P13). Regarding the different privacy states, participants appreciated the online-shared mode for the enhanced feature set (P3, P5, P6, P11). At the same time, they appreciated how easy the system made it to restrict access again, effectively giving them a sense of autonomy: *"Simply being able to just actively kick this thing out of the network so that it no longer has access to the devices, I think gives a very strong sense of security"* (P4). Participants emphasized that having the option to adjust privacy settings whenever they wanted to felt empowering (P1, P4): *"Just the fact that you have this range of options, where you can decide for yourself how much security is important to me personally, I think, also gives you a bit of security, because you have the feeling that you have it in your own hands and not that it's simply predetermined and you have to accept it"* (P4). Yet, three participants stated they had changed the privacy state only once and then just kept it as it was (P6, P8, P9). While some participants found the privacy states intuitive and easy to understand (P3, P10, P11), two participants stated that the wording of online and online-shared could be improved as they were initially confused about the difference between the two modes (P8, P10). Finally, we also asked participants whether they engaged with the history feature in the web app. Yet, most participants (P1, P3, P6, P8-P10, P13) did not engage with the history feature, and those that did use it mainly for activity insights, i.e., to see when which devices were active and track their own activity and behavioral patterns (P3, P4, P5). P10 stated that the history feature was not useful due to the limited study duration of one week but that they could imagine receiving a monthly summary might be helpful to optimize device usage or gain insights into privacy-sensitive devices.

5.1.3 Physical vs. Digital. In this theme, we report participants' discussions around the physical and digital aspects of the ecosystem and what they perceived as their strengths and weaknesses. The ecosystem allows users to control their devices and set the privacy states either digitally or physically by turning the proxies on the dashboard. Five participants preferred the digital (P1-P4, P6), and six participants the haptic interaction (P5, P7, P8, P10, P11, P13). In regards to the haptic interaction, participants liked that it felt more direct and easier as they could simply walk up to the board and turn the proxies instead of having to get their phone and pull up the website (P10-P13): *"It was simply quickest. Rather than taking out my phone, it was easier to just flip a switch"* (P13). Participants found this process especially tiresome outside of their homes, as the remote version of the web app required them to log in (P7, P10, P12, P13) and P13 even admitted that, despite considering themselves privacy-conscious, they did not change the privacy settings because they were too lazy to visit the website and log in. Here, participants suggested having an app instead of a website to reduce frequent logins and make the interaction more seamless (P3, P5, P8, P12, P13). In contrast, participants who preferred the digital interaction found it more convenient as they could remotely control devices and did not need to walk up the board. Three participants liked the haptic interaction as they considered it fun to use (P7, P9, P12), and P6 and P10 said they trusted the haptic interaction more to really deactivate a device or change a privacy state successfully: *"You can kind of, I don't know, flip the switch, like in a circuit breaker, and say, okay, now it's really off"* (P10). Moreover, P10 made changing privacy states part of their daily routine, and they emphasized how the physicality fits better into their workflow: *"When you put down your keys, put down your wallet, and then you can quickly use the knob, I think that's more in line with my personal workflow, [...] I think this is more my hardware workflow for when you're heading out."* Participants also discussed how the physical dashboard was especially helpful for visitors as it enabled them to directly see which devices were installed and in which mode they were in – something not possible with only a digital application (P1). In this regard, participants discussed how the dashboard triggered privacy-centered conversations with visitors (P11-P13): *"It definitely raised some questions, and I think for some people, it made them think, 'Okay, maybe I need to consider this more carefully"* (P11). Visitors of H6 not only asked questions about the board but actively engaged with it by changing states and triggering data flows. Participants also liked the physical dashboard as it had a single purpose and, thus, argued that the dashboard could not be simply replaced with a screen (P3, P8, P10, P12): *"I couldn't just ignore it. I liked this conscious connection"* (P3). However, many participants also found the dashboard in its current version too big and would only use it on a day-to-day basis if it was smaller (P1-P3, P6, P10-P13). Finally, participants argued that the digital and physical components complement each other nicely (P3-P5, P8-P13): *"I would like both. Because I don't always want to have a smartphone with me when I'm at home [...] but also when I'm away it would be cool if I forgot to change something to have access to it on my smartphone"* (P12).

5.2 Quantitative Results

We examined how often participants adjusted states and whether they used the physical or digital components. Additionally, we compared participants' responses to our self-defined questions before



(a) Digital vs. physical privacy change

(b) Chosen privacy states

(c) Total time per privacy state

Figure 9: (a) shows the frequency of households using the tangible dashboard and digital web application to adjust privacy states, (b) illustrates the privacy states to which devices were set, and (c) shows the total hours households spent in each state.

and after the study to assess the system's impact on their attitudes toward privacy and smart homes.

5.2.1 Private State Changes. We found that participants changed privacy states more frequently using the tangible dashboard ($N = 244$) than the web application ($N = 203$). Yet, reviewing households individually, we see stark differences, see Figure 9a. Three households (H1, H3, H4) changed the privacy state more often using the digital applications, and three households (H2, H5, H6) preferred the physical dashboard. The households most often set their devices to the online-shared state ($N = 202$), second most frequently to online ($N = 185$), and least often to local ($N = 154$). Yet, we also see that all states were used in each household, indicating that households switched between the different states depending on their needs, see Figure 9b. On average, households spent the most time in the online ($M = 230.76$ *hours*, $SD = 256.01$, $min = 28.63$, $max = 714.89$), followed by the online-shared ($M = 192.28$ *hours*, $SD = 283.97$, $min = 5.35$, $max = 761.66$), and the least amount of time in the local state ($M = 178.55$ *hours*, $SD = 159.19$, $min = 28.72$, $max = 471.80$). This indicates that, while there is a clear preference for certain states, there is significant variability in how long households kept devices in each state, see Figure 9c. For example, H2, despite most frequently switching to the online-shared state, remained in this state for only very short periods, likely switching to online-shared only when necessary.

5.2.2 System Usability Scale. We asked participants to rate the usability of the ecosystem's digital components (i.e., hub and web application) as well as the tangible dashboard. The tangible component received a mean rating of 79.38 ($SD = 12.93$) and the digital components a mean rating of 81.04 ($SD = 7.42$), indicating good usability of both systems according to established average values [1].

5.2.3 Participants' Attitude Towards Privacy and Smart Homes Before and After the Study. Next, we compared the participants' ratings of our self-defined questions ($Q_S1 - 8$) to investigate the impact of our ecosystem on participants' perception of privacy and smart homes, see Figure 10. The plot shows that while the perceived familiarity with smart home systems did not increase substantially (Q_S1), the ratings for the perceived importance of privacy (Q_S2), feeling of perceived control over privacy (Q_S5), knowledge of how to protect private data (Q_S7) and participants' perception of how well-informed they are about privacy-relevant processes in their smart home (Q_S8) increased considerably. At the same time, the ratings for the importance of the features (RQ_S3) or privacy (Q_S4) of a smart device decreased, as well as participants' worry about their private data in their smart home (Q_S6).

6 Discussion

To the best of our knowledge, PrivacyHub is the first functional prototype to provide cross-platform tangible privacy control features for both device users and bystanders. While prior work has explored the concept of tangible privacy, these efforts primarily focused on awareness features, such as a wooden dashboard [50], or were limited to mock-ups that precluded in-the-wild studies [15, 37, 42]. In contrast, our working prototype allowed us to gather real-world insights into people's lived experiences and perceptions of tangible privacy control coupled with awareness features. These insights are particularly valuable in privacy research, which often relies on online surveys and interviews without functional prototypes, making our findings potentially more robust and resistant to the privacy paradox [20].

In the following, we discuss how participants perceived the interaction with a privacy-centered interoperable smart home ecosystem and what role the tangible and digital features played in the interaction. Finally, we discuss how PrivacyHub increases awareness and control for smart home users.

6.1 From Burdensome Task to Daily Routine: The Hub as a Lever for Transforming Privacy Management

We explored how users perceive *privacy first* in their interactions with a cross-ecosystem smart home hub (**RQ1**). Our findings revealed that many participants integrated privacy management and decision-making into their daily routines. Participants noted that the ecosystem, particularly the dashboard, made managing privacy so easy and convenient that it no longer felt burdensome. Many even described interacting with the dashboard as fun and engaging. This is encouraging, as it highlights the ecosystem's potential to tackle the widely recognized privacy paradox, where users express concern for their privacy but fail to take steps to protect it [20]. Prior literature identifies complexity and effort as significant barriers to effective privacy management [22]. Universally available control hubs that seamlessly integrate into daily routines,

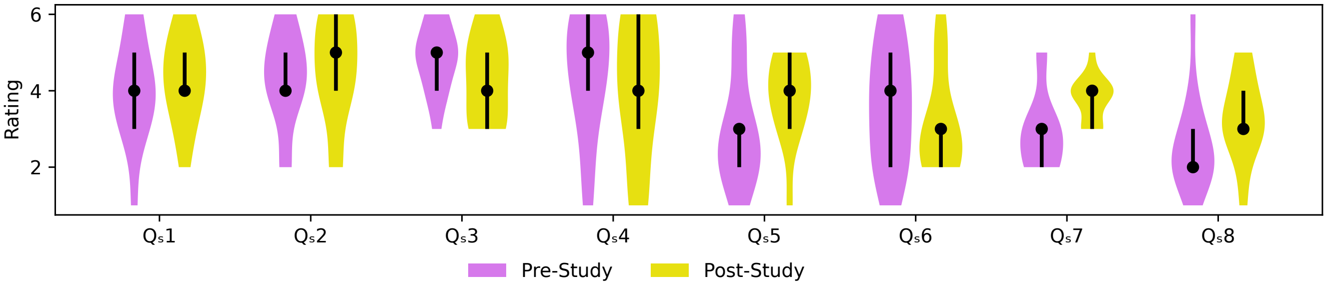


Figure 10: Ratings of Q_S1-8 before and after the study.

like the one studied here, could address this challenge. Participants also highlighted the importance of the dashboard's placement in supporting their workflow. Many participants found entering and leaving their apartments to be ideal moments for adjusting privacy states. Placing the board near the entrance could make this process more intuitive, allowing it to become part of their routine, much like grabbing their keys. In fact, the entrance area was already suggested by prior work as a suitable location for smart home privacy dashboards [50]. However, we observed that when privacy management did not align with a convenient moment, users often avoided it. Even self-identified privacy-conscious participants tended to forgo privacy management when it required too much effort. Here, an app instead of a website that does not require users to log in for every interaction can already be a suitable solution. In this regard, integrating privacy management features, such as connectivity control, into publicly available and frequently used apps, such as Apple's Home App, might be promising to foster active privacy engagement. *Overall, these insights show that when privacy management becomes seamless and effortless, it can become part of daily routines, removing some of the most prominent barriers to effective privacy protection: effort and complexity. However, achieving this requires that privacy tools support opportune moments and seamlessly blend into existing workflows.*

6.2 Strengthening the Case for Tangible Privacy: Physical Interaction as a Driver for Engagement

Our second research question revolved around how tangible and digital privacy features impact highly interoperable smart home systems (**RQ2**). In our study, the majority of participants preferred the tangible interaction as they characterized it as more direct, trustworthy, easy, and fun. Moreover, as we required participants to place the dashboard in a prominent location, they were constantly confronted with it, which reminded them to engage with privacy management. This is a unique advantage of the tangible compared to the digital component; since the digital application requires users to actively retrieve it, it cannot foster engagement when the user does not already intend to engage with privacy management. Moreover, the prominent placement provided a unique opportunity for bystanders to engage in privacy-related discussions. Prior work argued that bystanders need methods to engage with privacy as they often do not have similar opportunities as the device owner to act according to their privacy preferences or to engage with privacy regulations before being confronted with smart devices [30, 49]. Similar to prior work that found that privacy dashboards led to privacy discussions with bystanders [50], we also found that bystanders expressed interest and asked questions about the dashboard. Yet, in contrast to the dashboard from prior work, our tool allowed actual privacy control, leading to bystanders not only expressing interest but also actively engaging with the dashboard by changing states and triggering visualization flows. It would be interesting for future work to observe whether bystanders actually act according to their preferences and adjust privacy states or if they would avoid the social conflict as suspected by Windl et al. [50]. If this were the case, such a privacy hub might be especially valuable in a scenario where the bystander does not have direct contact with the device owner, such as in short-term rental scenarios. Indeed, our hub might fulfill the need identified by Mare et al. [34]: *"We propose creating a smart home dashboard for guests. Such a dashboard could show guests relevant information about the devices in the Airbnb and provide an interface to control them."*

While we found differences in individual preferences, with some participants preferring the tangible and others preferring the digital interaction, we could not necessarily relate this to participants' tech-savviness, i.e., to their ATI score or whether they self-identified as pilot or passenger users. This stands in contrast to related work that argues that a higher technical affinity comes with a higher preference for tangible mechanisms [13]. Here, Delgado Rodriguez et al. [13] further argue that their findings challenge prior work's suggestions to develop tangible mechanisms, especially for non-tech-savvy groups or the elderly. While our findings should be interpreted cautiously due to the limited sample size, our work indicates that the investigation of tangible mechanisms benefits from lived experiences as they may need to be experienced firsthand to be fully understood – especially by the less tech-savvy population.

While we found strong arguments for tangible interaction, participants highlighted that the digital app complemented the system effectively. They used it as a remote control when they were out of reach of the dashboard or when they were outside the house, making interaction with the physical board impossible. This suggests that tangible privacy controls should not replace digital alternatives; instead, both need to coexist, each contributing its own strengths.

Our findings strengthen the argument for tangible privacy. Not only did the majority prefer interacting with the tangible dashboard, *but it also fostered engagement through direct, trustworthy, and fun interactions. This not only encouraged device owners to manage privacy but also enabled bystanders to participate in privacy-centered discussions. Further, our results suggest that tangible mechanisms might need to be experienced first-hand to be fully understood, especially by a less tech-savvy population. Despite these strong arguments for tangibility, we recognize the value of supplementing physical with digital components to ensure an effective and user-friendly ecosystem. Offering both tangible and digital mechanisms by leveraging their individual strengths further contributes positively to the call for inclusive privacy [50].*

6.3 PrivacyHub: Increasing Awareness and Control Through a Cross-Device Smart Home Ecosystem

The dashboard's prominent placement, combined with data flow visualizations, encouraged continuous privacy reflection and raised users' privacy awareness. Participants noted that the flow visualizations helped them understand their devices' internal states and processes, increasing their awareness of data being sent and processed. This insight is significant for future research, as previous studies have explored privacy data visualizations in smart homes [6, 41], but none have directly examined their impact on users' understanding and awareness of privacy-relevant processes. The hub provided a visual awareness signal by flashing in the respective color whenever a privacy state was adjusted, alerting co-inhabitants to digital changes. Users appreciated this feature as it allowed them to reassess their comfort in real-time and adjust their privacy settings as needed, effectively enhancing their privacy autonomy. Questionnaire results reinforced findings from the interviews: Participants rated their perceived importance of privacy higher post-study, indicating that the system effectively increased their awareness. Further, they rated their perception of how well-informed they are about privacy-relevant processes more positively, indicating that the data flows fulfilled their educational purpose. The control features further enhanced participants' sense of agency, as they reported greater perceived control and knowledge of how to protect their private data. Simultaneously, their concerns about private data in smart homes decreased, along with the perceived importance of device privacy features, suggesting a more balanced perspective. These findings align with research on interactive privacy labels, which show that visualizing privacy/feature trade-offs helps users make informed decisions [46]. Our findings suggest a similar effect, promoting a more balanced perspective on smart devices and indicating that a smart home hub could facilitate smart device adoption by reducing concerns and reshaping users' priorities. *The hub enhanced users' privacy awareness and perceived control, granting them greater autonomy over their privacy. Additionally, it could benefit device manufacturers by encouraging smart device adoption, ultimately making our findings valuable for both privacy research and industry development.*

6.4 Interoperability As Vehicle for Privacy

The digital and tangible privacy tools developed as part of PrivacyHub could ultimately be paired with any number of existing proprietary and non-proprietary smart home ecosystems. Such integrations would require individual adaptation to single manufacturers or ecosystems and protocols (e.g., Apple HomeKit, Amazon Alexa, or Google Home). We argue that our findings on privacy tools are valuable and relevant to the broader field of smart home privacy research and development. We emphasize that the ability to integrate our privacy tools with technologies and protocols like Matter and Thread, which enable smart home interoperability, provides a timely and unique perspective. Our work showed that users largely overlooked the complexities of differing device types, sensing capabilities, and manufacturers. Instead, they intuitively engaged with smart devices through unified digital and tangible privacy interfaces. This seamless interaction allowed them to easily navigate new smart home paradigms, such as connectivity control and data transmission visualization. These findings highlight not only the value of interoperability for simplifying smart home setup and operation but also its critical role as a foundation for effective privacy management. While it would be ideal for commercial Matter hubs to support similar privacy features, such functionality is currently unavailable, and there is no indication that manufacturers are working towards implementing it. Even if they could do so, the question arises whether they would also choose to extend these features to devices from other manufacturers. We developed PrivacyHub independently, without industry dependencies, allowing us to focus on creating user-centric privacy features. Based on our findings, we strongly advocate for other hubs to adopt interoperable privacy features to promote transparency and control across smart home ecosystems. Introducing consistent privacy interfaces across manufacturers and device types will strongly help to push the availability of privacy tools in smart homes. In this context, we note that we do not aim to prescribe the exact same set of tangible and digital tools as a reference implementation for future interoperable smart homes. *Rather, we argue for cross-ecosystem hubs to offer a range of privacy tool options that follow established UX and interaction concepts. Smart home users can then decide which privacy tools to add and combine in their homes, carrying the concept of interoperability from smart home devices all the way to privacy awareness and management tools.*

6.5 Limitations and Future Work

We designed PrivacyHub to provide granular network control and raise privacy awareness through data flow visualization. However, the system does not currently include functionality for monitoring or controlling network traffic, such as ARP spoofing or other traffic interception techniques [24]. This design choice was intentional, as we focused on offering transparent and tangible control over devices rather than implementing advanced security features. Yet, future iterations could integrate these features to enhance security, ideally in collaboration with IT security specialists.

The technical complexity of our ecosystem limited us to a single prototype, refined to operate error-free and without researcher involvement over extended periods. This restriction slowed the study, as we could test only one household at a time, resulting in a small sample size. Convenience sampling further constrained the participant pool to nearby individuals, skewing the sample toward younger, more educated users. While this impacts generalizability, the in-the-wild study provided unique insights into users' lived experiences and behaviors, which are challenging to capture in lab settings. Future studies should include a larger and more diverse sample to enhance generalizability.

The study's one-week duration, common in similar HCI research [9, 23, 47], may have led to a novelty effect. Participants found the system engaging but noted that features like data flow visualizations might feel repetitive over time. However, they suggested that functions like the history feature could reveal greater value over extended use. Future research with a longer study duration could better evaluate the system's long-term utility.

Currently, our prototype supports only a limited set of devices, which are not among the most privacy-sensitive, such as microphones and cameras [49]. While Matter-enabled devices offer advanced encryption and interoperability, the standard does not dictate privacy practices, and participants were likely unaware of its benefits. Therefore, we do not believe Matter introduced bias into their privacy perceptions. However, limiting the study to Matter-supported devices may impact the generalizability of our findings. Future iterations should integrate a broader range of devices, including more privacy-sensitive ones, to provide a more comprehensive evaluation of privacy concerns.

Our system also does not yet provide granular privacy controls for individual sensors, such as disabling a smart speaker's microphone while allowing it to play music. This limitation exists because current devices lack hardware or API support for sensor-level adjustments. Incorporating such features in the future would greatly enhance the system by addressing users' diverse privacy concerns regarding different sensor types [49]. Adding simple on/off controls alongside connectivity management could further improve the system's adaptability to diverse privacy needs.

Another limitation was the inability to integrate participants' existing smart home devices. Due to the early development stage of the Matter standard, which supports only a limited range of devices, we selected three sample devices for the study. While this provided valuable insights by enabling real interaction, the experience would have been more natural if participants used their own devices, which are already part of their routines. Future research should revisit this approach as Matter matures and supports more devices.

Our dashboard was relatively large, a design choice that some participants criticized, with several suggesting they would prefer a smaller version. We opted for this size in response to recent calls for more inclusive smart home privacy [50], aiming to enhance usability for visually impaired individuals and the elderly. However, we recognize that a smaller size could also be beneficial, as it would make the dashboard easier to integrate into a home environment. Therefore, future iterations of the dashboard should be available in multiple sizes to accommodate diverse user needs.

7 Conclusion

We built a functional smart home cross-device privacy hub featuring a smart home hub, a tangible dashboard, and a web application. The system provides control by allowing the adjustment of privacy states and raises awareness by visualizing data flows. By deploying the dashboard in six households and with 13 participants over one week, we found that the system effectively raised participants' privacy awareness and feeling of control, led to more privacy-driven decisions, and enhanced their understanding of privacy-relevant processes. We further found that most participants preferred changing privacy states through the haptic interaction, even though this preference varied by participant. Participants especially appreciated the haptic interaction for being more direct and trustworthy and providing continuous reflections, which was also beneficial for bystanders as it allowed them to engage in privacy-focused discussions. Finally, we saw how participants successfully integrated the privacy hub into their daily routines, eventually transforming privacy management from a burdensome task to part of their routines. We, thus, conclude that cross-ecosystem hubs can contribute to effective privacy management and emphasize the role of interoperability as a vehicle for the wider accessibility of privacy awareness and control in smart homes.

References

[1] Philip T. Kortum Aaron Bangor and James T. Miller. 2008. An Empirical Evaluation of the System Usability Scale. *International Journal of Human–Computer Interaction* 24, 6 (2008), 574–594. doi:10.1080/10447310802205776

[2] Luca Hernández Acostsa and Delphine Reinhardt. 2022. Multi-User Privacy with Voice-Controlled Digital Assistants. In *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*. 30–33. doi:10.1109/PerComWorkshops53856.2022.9767270

[3] 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. doi:10.1145/3415187

[4] Ahmed Alshehri, Joseph Spielman, Amiya Prasad, and Chuan Yue. 2022. Exploring the Privacy Concerns of Bystanders in Smart Homes from the Perspectives of Both Owners and Bystanders. (2022). doi:10.56553/popets-2022-0064

[5] 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).

[6] Carlos Bermejo Fernandez, Petteri Nurmi, and Pan Hui. 2021. Seeing is Believing? Effects of Visualization on Smart Device Privacy Perceptions. In *Proceedings of the 29th ACM International Conference on Multimedia* (Virtual Event, China) *(MM '21)*. Association for Computing Machinery, New York, NY, USA, 4183–4192. doi:10.1145/3474085.3475552

[7] Ann Blandford, Dominic Furniss, and Stephann Makri. 2016. *Qualitative HCI Research: Going Behind the Scenes*. Springer Cham, Cham, Switzerland. 51–60 pages. doi:10.2200/S00706ED1V01Y201602HCI034

[8] John Brooke. 1996. SUS: A Quick and Dirty Usability Scale. In *Usability Evaluation in Industry*, Patrick W. Jordan, Bruce Thomas, Bernard A. Weerdmeester, and Ian L. McClelland (Eds.). Taylor & Francis, Chapter 35, 189–194. doi:10.1201/9781498710411-35

[9] Barry Brown, Fanjun Bu, Ilan Mandel, and Wendy Ju. 2024. Trash in Motion: Emergent Interactions with a Robotic Trashcan. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 591, 17 pages. doi:10.1145/3613904.3642610

[10] 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. doi:10.1109/EISIC.2016.044

[11] 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. 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 555, 16 pages. doi:10.1145/3411764.3445691

[12] 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. doi:10.1145/3313831.3376304

[13] Sarah Delgado Rodriguez, Priyasha Chatterjee, Anh Dao Phuong, Florian Alt, and Karola Marky. 2024. Do You Need to Touch? Exploring Correlations between Personal Attributes and Preferences for Tangible Privacy Mechanisms. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 981, 23 pages. doi:10.1145/3613904.3642863

[14] 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. doi:10.18420/muc2021-mci-ws09-393

[15] 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 *Nordic Human-Computer Interaction Conference* (Aarhus, Denmark) *(NordiCHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 74, 13 pages. doi:10.1145/3546155.3546640

[16] 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. doi:10.1145/3494983

[17] Sebastian S. Feger, Maximiliane Windl, Jesse Grootjen, and Albrecht Schmidt. 2023. ConnectivityControl: Providing Smart Home Users with Real Privacy Configuration Options. In *End-User Development: 9th International Symposium, IS-EUD 2023, Cagliari, Italy, June 6–8, 2023, Proceedings* (Cagliari, Italy). Springer-Verlag, Berlin, Heidelberg, 180–188. doi:10.1007/978-3-031-34433-6_11

[18] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A personal resource for technology interaction: development and validation of the affinity for technology interaction (ATI) scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467. doi:10.1080/10447318.2018.1456150

[19] Christine Geeng and Franziska Roesner. 2019. Who's In Control? Interactions In Multi-User 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, 1–13. doi:10.1145/3290605.3300498

[20] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security* 77 (2018), 226–261. doi:10.1016/j.cose.2018.04.002

[21] 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

[22] Nina Gerber, Verena Zimmermann, and Melanie Volkamer. 2019. Why Johnny Fails to Protect his Privacy. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 109–118. doi:10.1109/EuroSPW.2019.00019

[23] Luke Haliburton, Maximilian Lammel, Jakob Karolus, and Albrecht Schmidt. 2022. Think Inside the Box: Investigating the Consequences of Everyday Physical Opt-Out Strategies for Mindful Smartphone Use. In *Proceedings of the 21st International Conference on Mobile and Ubiquitous Multimedia* (Lisbon, Portugal) *(MUM '22)*. Association for Computing Machinery, New York, NY, USA, 37–46. doi:10.1145/3568444.3568452

[24] Danny Yuxing Huang, Noah Apthorpe, Frank Li, Gunes Acar, and Nick Feamster. 2020. IoT Inspector: Crowdsourcing Labeled Network Traffic from Smart Home Devices at Scale. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 4, 2, Article 46 (June 2020), 21 pages. doi:10.1145/3397333

[25] Hilary Hutchinson, Wendy Mackay, Bo Westerlund, Benjamin B. Bederson, Allison Druin, Catherine Plaisant, Michel Beaudouin-Lafon, Stéphane Conversy, Helen Evans, Heiko Hansen, Nicolas Roussel, and Björn Eiderbäck. 2003. Technology probes: inspiring design for and with families. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Ft. Lauderdale, Florida, USA) *(CHI '03)*. Association for Computing Machinery, New York, NY, USA, 17–24. doi:10.1145/642611.642616

[26] 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. doi:10.1145/3491102.3517602

[27] 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. doi:10.1145/3461778.3462073

[28] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. 2021. "We Just Use What They Give Us": Understanding Passenger User Perspectives in Smart Homes. 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 41, 14 pages. doi:10.1145/3411764.3445598

[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. doi: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. doi:10.1145/3274371

[31] Roxanne Leitão. 2019. Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse. 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. doi:10.1145/3322276.3322366

[32] 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*. doi:10.14722/eurousec.2018.23016

[33] 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). doi:10.2478/popets-2019-0068

[34] 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. doi:10.2478/popets-2020-0035

[35] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You just can't know about everything": Privacy Perceptions of Smart Home Visitors. In *Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia* (Essen, Germany) *(MUM '20)*. Association for Computing Machinery, New York, NY, USA, 83–95. doi:10.1145/3428361.3428464

[36] 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. doi:10.1145/3419249.3420164

[37] 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. doi:10.1145/3430506

[38] 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. doi:10.1145/1878431.1878446

[39] 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. doi:10.1145/1409635.1409661

[40] 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. doi:10.1145/2899007.2899008

[41] Sarah Prange, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. 2021. PriView– Exploring Visualisations to Support Users' Privacy Awareness. 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 69, 18 pages. doi:10.1145/3411764.3445067

[42] Parth Kirankumar Thakkar, Shijing He, Shiyu Xu, Danny Yuxing Huang, and Yaxing Yao. 2022. "It would probably turn into a social faux-pas": Users' and Bystanders' Preferences of Privacy Awareness Mechanisms in Smart Homes. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 404, 13 pages. doi:10.1145/3491102.3502137

[43] Philipp Thalhammer, David Müller, Alexander Schmidt, Michael Huber, Albrecht Schmidt, and Sebastian Feger. 2023. ConnectivityControl: A Model Ecosystem for Advanced Smart Home Privacy. In *Proceedings of the 22nd International Conference on Mobile and Ubiquitous Multimedia* (Vienna, Austria) *(MUM '23)*. Association for Computing Machinery, New York, NY, USA, 556–558. doi:10.1145/3626705.3631876

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

[45] Ishaq Unwala, Zafar Taqvi, and Jiang Lu. 2018. Thread: An IoT Protocol. In *2018 IEEE Green Technologies Conference (GreenTech)*. IEEE, Austin, TX, 161–167. doi:10.1109/GreenTech.2018.00037

[46] Maximiliane Windl and Sebastian S. Feger. 2024. Designing Interactive Privacy Labels for Advanced Smart Home Device Configuration Options. In *Proceedings of the 2024 ACM Designing Interactive Systems Conference* (Copenhagen, Denmark)

(DIS '24). Association for Computing Machinery, New York, NY, USA, 3372–3388. doi:10.1145/3643834.3661527

[47] 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. doi:10.1145/3491102.3517688

[48] 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. doi:10.1145/3567739

[49] 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. doi:10.1145/3546719

[50] 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* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 70, 16 pages. doi:10.1145/3544548.3581167

[51] Peter Worthy, Ben Matthews, and Stephen Viller. 2016. Trust Me: Doubts and Concerns Living with the Internet of Things. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems* (Brisbane, QLD, Australia) *(DIS '16)*. Association for Computing Machinery, New York, NY, USA, 427–434. doi:10.1145/2901790.2901890

[52] 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. doi:10.1145/3290605.3300428

[53] 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. doi:10.1145/3359161

[54] Wondimu Zegeye, Ahamed Jemal, and Kevin Kornegay. 2023. Connected Smart Home over Matter Protocol. In *2023 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, Las Vegas, NV, USA, 1–7. doi:10.1109/ICCE56470.2023.10043520

[55] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 65–80. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

[56] 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. doi:10.1145/3274469

A Appendix

A.1 Questionnaire

A.1.1 Demographics.

Q_D1 How old are you?
Q_D2 Which gender do you most identify with?
Q_D3 What is your current primary occupation?
Q_D4 What is the highest degree you have received?
Q_D5 How many smart devices are in your household?

A.1.2 User Type.

Q_U1 Please indicate which user group you identify with more.
Pilot user: A user who is responsible for installing, configuring, and regularly using smart devices in the home as part of their everyday life.
Passenger user: A user whose daily life is influenced by smart devices in their home—either through their own use or through the use of someone else—but who has not set up or configured the devices themselves.
Please indicate which user type applies to you.

A.1.3 Smart Home Experience and Privacy Awareness.

Q_S1 I am very familiar with smart home systems.
Q_S2 Privacy is very important to me.
Q_S3 The features of a smart device are my top priority.
Q_S4 Privacy protection is my top priority when choosing a smart device.
Q_S5 I feel in control of my private data in my smart home.
Q_S6 I worry a lot about my private data in my smart home.
Q_S7 I know how to protect my private data in my smart home.
Q_S8 I feel well-informed about what happens to my private data in my smart home.
Q_S9 How often do you use smart home devices?

A.1.4 Interview Questions.

Q_I1 Which feature of the system did you use the most?
Q_I2 When did you make changes to the privacy states? Why?
Q_I3 How intuitive was it for you to set privacy states for different devices? Why?
Q_I4 Where did you mostly configure the privacy states (web application vs. tangible dashboard)? Why?
Q_I5 How has your awareness or attitude toward privacy changed through your interaction with the system?
Q_I6 Would you use the system in your daily life (outside of the study context)? Why? Which parts of it?
Q_I7 Would you recommend the system to your friends or family? Why or why not?
Q_I8 Did you encounter any issues while using the system? If yes, which ones?
Q_I9 How secure (in terms of privacy) did you feel when using the system?
Q_I10 What additional features would you like the system to have?
Q_I11 Has the system helped you make better decisions regarding privacy in your smart home? If so, how?
Q_I12 How did you perceive the interaction with the website?
Q_I13 How did you perceive the visualizations of the LED ring?
Q_I14 When did you use the online website, and why?
Q_I15 What insights did you gain from the history feature?
Q_I16 Did you connect a third-party hub to the system? What were your experiences with this feature?
Q_I17 What would you improve about the hub?
Q_I18 How did you perceive the tangible interaction with the dashboard? Do you find a tangible or a purely digital experience more comfortable? Or a mix of both?
Q_I19 How did you perceive the visual representation of data flows on the dashboard?
Q_I20 How did the visualizations of data flows on the dashboard affect your perception of privacy?
Q_I21 How helpful was the dashboard in managing and monitoring your smart home?
Q_I22 What would you improve about the dashboard?
Q_I23 Do you have any other comments?