PriKey – Investigating Tangible Privacy Control for Smart Home Inhabitants and Visitors

Sarah Delgado Rodriguez
University of the Bundeswehr Munich
Germany
sarah.delgado@unibw.de

Sarah Prange
University of the Bundeswehr Munich
LMU Munich
Germany
sarah.prange@unibw.de

Christina Vergara Ossenberg
Technical University Darmstadt
Germany
christina.vergaraossenberg@stud.tu-darmstadt.de

Markus Henkel
Technical University Darmstadt
Germany
markus.henkel@stud.tu-darmstadt.de

Florian Alt
University of the Bundeswehr Munich
Germany
florian.alt@unibw.de

Karola Marky
Leibniz University Hannover
Germany
University of Glasgow
UK
karola.marky@itsec.uni-hannover.de

Figure 1: We present *PriKey*, a concept for tangible smart home privacy mechanisms that enable smart home inhabitants and visitors alike to communicate and execute their privacy choices. It reduces complexity by grouping privacy choices by sensor type (i.e., video, audio, and presence sensing) and room (e.g., kitchen) instead of single devices.

ABSTRACT

The increasing number of smart devices installed in our homes poses privacy risks for inhabitants and visitors. However, individuals face difficulties counteracting privacy intrusions due to missing controls, incorrect mental models, and limitations in their level of expertise. We present *PriKey*, a concept for device-independent and easy-to-use tangible smart home privacy mechanisms. *PriKey is the key to privacy protection*: it supports users in taking control over their privacy through meaningful, tangible interactions. Using a Wizard-of-Oz prototype, we explored users' perceptions regarding *PriKey* ($N = 16$). We then compared *PriKey* to an equivalent smartphone app ($N = 32$), focusing on visitors. Participants perceived *PriKey* as engaging, intuitive, and benevolent. Their privacy considerations were based on personal and contextual factors. While most participants preferred the smartphone app, others clearly favored *PriKey*. Our results indicate that tangible privacy is a noteworthy approach for future smart home privacy mechanisms.

CCS CONCEPTS

• **Security and privacy** → **Usability in security and privacy**; • **Human-centered computing** → *Ubiquitous and mobile devices.*

KEYWORDS

smart home, privacy, tangible, tangible privacy, privacy assistance, bystander

ACM Reference Format:
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 (NordiCHI '22), October 8–12, 2022, Aarhus, Denmark.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3546155.3546640

NordiCHI '22, October 8–12, 2022, Aarhus, Denmark

ACM ISBN 978-1-4503-9699-8/22/10…$15.00
https://doi.org/10.1145/3546155.3546640

1 INTRODUCTION

Smart devices have been increasingly adopted in our most private environment: our homes. On top of the omnipresent smartphones, sensor-enhanced and connected devices, such as lights, smart speakers, TVs, or vacuum cleaners, are ubiquitous parts of the modern lifestyle. Their built-in sensors, like microphones, cameras, or presence sensors, impose a privacy risk, as such devices potentially collect sensitive data of nearby individuals and may share it with manufacturers or third parties [2, 47]. While primary users of these devices might be aware of possible privacy risks, co-inhabitants and visitors often lack this knowledge [56, 62]. Hence, recent scientific work identified a need for usable and transparent smart home privacy choice mechanisms for multiple user types, including *inhabitants* and *visitors* [1, 40, 62, 63]. Suggested approaches, however, frequently suffer from adoption barriers and mistrust, especially for visitors and less experienced or less tech-savvy individuals [1, 20, 21, 31, 46, 50]. Those are rooted in the excessive complexity, non-intuitive and non-engaging interactions of such software-based mechanisms.

To enhance the privacy of individuals in smart environments, related work conceptualized the term *tangible privacy*, which designates systems allowing users to manage their privacy settings through direct and tangible interactions [1, 46]. However, *tangible privacy mechanisms* targeting more than a specific device have rarely been investigated, especially not through the implementation of prototypes. To close this gap, we present *PriKey*, a concept for *device-independent and uncomplex, tangible privacy mechanisms* for smart homes. To render our concept comprehensible for end-user evaluation purposes, we implemented a Wizard-of-Oz prototype (see Figure 1).

We conducted an exploratory user study ($N = 16$), where participants interacted with *PriKey* in different scenarios, investigating the following *research questions*:

- **RQ1 - Perception of PriKey:** What are users' perceptions of *PriKey*, in particular:
  RQ1.1 Interaction with *PriKey*: How do users perceive the interaction with *PriKey*?
  RQ1.2 Broader Implications: What are the broader implications of *PriKey*?
- **RQ2 Privacy Considerations:** What are users' specific privacy considerations when using *PriKey*?

We found that participants appreciated the intuitive, engaging, and meaningful interactions supported by *PriKey*. Furthermore, we identified personal factors that influence participants' privacy considerations, such as their roles, risk perceptions, or current context (i.e., main task, intimacy and familiarity of the environment, installed devices). In a second remote study ($N = 32$), we compared *PriKey* to a smartphone app with similar capabilities (as this is currently state-of-the-art [18, 29]), focusing on visitors:

- **RQ3 Comparison:** How do visitors in unfamiliar environments perceive *PriKey* compared to a mobile app?

Participants' preferences regarding *PriKey* and the smartphone app were divided. While most participants of both user studies would prefer the app on a smartphone they already have, others strongly favored *PriKey* as they perceived it more benevolent, direct and ready-to-hand.

Our work can serve as a stepping-stone for future research on tangible privacy mechanisms. We argue that privacy controls for smart homes should incorporate possibilities for personal choices and preferences by-design, rather than one-fits-all approaches. This especially applies to users' favored interaction modalities and form factor. This would lead to better user experiences and, ultimately, to enjoyable, usable and trusted privacy controls for individuals.

2 BACKGROUND & RELATED WORK

We build on several strands of related work: privacy challenges and mechanisms for smart homes, and tangible privacy.

2.1 Privacy Challenges in Smart Homes

The investigation of privacy aspects in smart homes in prior work revealed three major privacy challenges [8, 36, 38, 57, 63, 64]:

2.1.1 Multi-User Environments. Smart homes are multi-user environments: *primary users* install, own, and administer smart home devices, while *co-inhabitants*, e.g., inhabitants that live in the smart home, use devices while not administering them. In contrast, *visitors* might not even know about installed devices [62]. Even though smart home devices are often considered as inherently shareable "family devices", individuals distinguish between primary users and co-inhabitants [21], resulting in a power imbalance as co-inhabitants and visitors frequently cannot change privacy settings [22, 29]. Visitors and co-inhabitants want to be aware of smart home devices in their environment or even control data collection themselves, e.g., by switching devices off [41]. However, co-inhabitants and visitors might be reluctant to control others' devices due to social awkwardness, and cooperative solutions might be preferred [62]. Moreover, privacy settings can be negotiated over time [22] and are influenced by social relations [11, 61].

2.1.2 Awareness. A prerequisite for making informed privacy choices is *awareness* of data collection and processing [40]. Awareness, however, varies largely between different individuals based on their level of expertise [53], experience [40], or risk perceptions [63]. While inhabitants of smart homes can gain awareness over time, visitors might lack knowledge of the devices in their environment [40, 62]. Furthermore, visitors find it difficult to interpret devices' current states and capabilities that might influence their privacy choices [1].

Specific methods for increasing inhabitants' and visitors' awareness include privacy labels on devices' packaging [17, 32]; device locators in the form of LEDs [56]; QR codes that link further information on devices [62]; systems that allow to detect and physically localize wireless monitoring devices [55]; educational approaches [54]; or visualizing spaces of data tracking by means of augmented reality [50].

2.1.3 Control. The third and last privacy challenge is enabling control over the data collection, i.e., enforcing the privacy decision. It has been shown that all types of individuals that can be present in a smart home wish to control or at least consent to data collection [41, 49, 61–64]. Zeng and Roesner found that implementing access control is challenging in smart homes due to the complex role system [63]. Their prototype system was rarely used, as it was perceived as too complex and conflicted with social norms, trust,

and respect. Another aspect of the control challenge is related to the multi-user aspects: co-inhabitants or visitors might overwrite the settings of primary device users. Hence, related work recommended guest modes that preserve primary users' privacy [18, 34, 41, 63]. However, this requires co-inhabitants and visitors to interact with devices to configure privacy settings before the devices can be used. As most available smart home devices have hidden control interfaces or require a smartphone app, exerting control for co-inhabitants and visitors is challenging [29].

2.2 Privacy Mechanisms for Smart Homes

To address privacy challenges in smart homes, researchers suggested developing *privacy mechanisms* supporting users in making and enforcing personal privacy choices [14, 53]. Such systems (a) enhance awareness on nearby devices and (b) enable control over them to avoid privacy invasions [13, 14]. However, smart home privacy mechanisms frequently suffer from usability and trust issues, as well as excessive complexity, especially for less tech-savvy or experienced users and for the increasing number of devices [13, 53]. He et al. proposed a privacy settings interface supporting individuals in configuring their smart environments in a privacy protecting manner [30]. Seymore et al. extended this interface by offering a firewall to prevent data leakage [53]. Moreover, software-based privacy mechanisms might not give adequate feedback about the device state and individuals even mistrust them, but instead prefer tangible control and feedback features [1], which motivates *PriKey*.

2.3 Tangible Privacy Mechanisms

Tangibles are physical objects for manipulating digital data [51]. Compared to software-based solutions, tangibles can enhance usability, feedback, and availability for less tech-savvy users [43]. *Tangible privacy mechanisms* should enable unambiguous communication and control of states, and capabilities of smart home devices [1]. They can reduce the complexity and enhance the naturalism of interactions, feedback, and social compatibility [43].

Mehta et al. [46] proposed *Privacy Care*, a framework for tangible and embodied privacy management, addressing control and awareness challenges (cf. Sections 2.1.2 and 2.1.3). They argue that privacy mechanisms should be (a) *embodied* (i.e., integrated in everyday environments and objects), (b) *direct* (i.e., timely and intuitive action and feedback), (c) *ready-to-hand* (i.e., embedded in the environment or task and granularity adapting to users' attention), and (d) *customizable* for different contexts (i.e., modular hardware, configurable software). Users prefer physical attributes for awareness features and spatial movement for privacy controls [45], which inspired our prototype.

Many tangible privacy prototypes target *one specific device or sensor type*. Examples are wearables, allowing control over potential location tracking [44] or jamming (hidden) microphones [10]. The "privacy hat" can mute a smart speaker's microphone [58]. "Posit", a smart calendar, only visualizes private data when it is located in a private environment [33]. Another example for tangible privacy controls are (smart) webcam covers [16]. In contrast, the *PriKey* concept aims at exerting device- and sensor-independent control.

3 THE *PRIKEY* CONCEPT

From the literature, we derived the following basic requirements and design considerations for the *PriKey* concept:

Device-Independence. Our mechanism should not be restricted to specific devices or sensors, but be generally applicable to *different types of smart home devices* (e.g., thermostats, smart speakers, or security cameras) that also integrate *diverging sensors* (e.g., presence, audio, and video). We investigated the capabilities of widely used consumer smart home devices. We extracted the top 50 smart home bestseller list from a leading online marketplace and gathered details on each device (cf. Supplementary Material A). The most common sensors are microphones (14 devices), video cameras (10), and presence sensors (9). *PriKey* should enable control of smart home devices using these sensors.

Sensor-Based and User-Centric Control. PriKey should offer scalable and uncomplex privacy control, considering environments with multiple devices. Most privacy mechanisms allow controlling each device independently [18, 53], which leads to an increase in the amount of information and required privacy decisions with an increasing number of devices. This is further aggravated when devices that are not in the vicinity of the user are included, even though they do not pose privacy threats. To reduce the complexity of privacy control for multiple smart home devices, we approach scalability from a new perspective by *grouping different privacy choices by type of sensor*. With *PriKey*, users can choose to allow or reject all video, audio, or presence recordings of nearby devices independently. This means that *PriKey* deactivates integrated sensors only, not complete devices. Hence, devices could still provide other functionalities and be controlled through non-related interfaces (e.g., a smartphone app instead of voice control). *PriKey* also allows to directly prohibit all types of data collection from nearby devices. Furthermore, we divided the space within the smart home into intuitively comprehensible units, namely its rooms. *PriKey*-supported privacy choices target *all smart home devices that are situated inside the room where the user is currently located.* Thus, when we mention "nearby device" in the following, we mean all devices installed in the actual room. Smart homes are usually indoor spaces, which makes this decision possible. However, it is not applicable to not clearly delimited spaces, where a fixed user-centric range could be used as a fallback method.

Tangibility. Tangible interactions enable *direct, integrated* and *meaningful* control and communication of data [59], making them the ideal basis for both, awareness and control functionalities of privacy mechanisms [45, 46]. Tangible mechanisms materialize the abstract concept "privacy" by making it physically graspable and directly manipulable. Therefore, they could support mental models and reduce cognitive load [15, 46]. Hence, *PriKey* enables tangible interactions by using dedicated hardware controls, such as buttons or switches, to immediately (de-)activate the data collection of nearby sensors. Moreover, *PriKey* provides clear and unambiguous feedback [1]. Configured privacy decisions are consistent, meaning that they apply to any device until they are modified. This enables proactive privacy control: users can set their preferred configurations before even entering a specific smart environment. *PriKey*'s control features are always at hand in the form of a mobile gadget.

Equalize Power Imbalances. *PriKey* should equally consider *all involved individuals* in a smart home. Based on related work, we distinguish two levels of familiarity for visitors: familiar and unfamiliar [50]. Correspondingly, *involved individuals* include primary users, co-inhabitants, visitors in familiar environments, and visitors in unfamiliar environments. Our system allows for privacy settings to be applied to all devices in the environment – regardless of how many devices there are and where. This supports users who lack expertise in using smart home devices or who cannot access them due to physical, technological, or social limitations. Moreover, *PriKey* deactivates all sensors of a specific type, if *any* involved individual configures their system correspondingly. This ensures that devices do not perform undesired collection of personal data, further equalizing existing power imbalances.

4 WIZARD-OF-OZ PROTOTYPE OF *PRIKEY*

Our implementation of *PriKey* includes 1) the *PriKey-tangible* to execute privacy decisions in a straightforward manner, including immediate feedback on the effects on nearby device sensors; 2) the *PriKey-station* for more detailed and transparent information. Since our research focuses on users' perception of *PriKey*, rather than on the implementation of privacy controls, our prototype does not provide actual control over sensors, but we simulate this part in our study.

4.1 PriKey-Tangible

To evaluate our concept, we implemented a lightweight and robust *PriKey-tangible*.

Features & Components. Based on the findings from Mehta et al. [45], we considered incorporating attribute-related feedback (e.g., cold-warm or dark-bright) for awareness features and force (e.g., block, enable, resist) or space (e.g., near-far, up-down, forward-backward) related interactions for control. Hence, we integrated green *light emitting diodes* (LEDs) (i.e., attributes: dark-bright) into our *tangible* to communicate the *states of the different sensor groups* (i.e., presence, audio, and video) of nearby devices. We also chose switches (i.e., actuated by the *key teeth sliders*) for implementing the control features since they represent force and space-related interactions and provide well-known and intuitive means of tangible input. All components were supplied through a 3 volt battery and controlled by an ATtiny 84a microcontroller. To provide users the possibility to turn off all nearby sensors immediately, we incorporated an *All Off* button with a state-communicating red LED.

Design & Functionalities. Our prototype is shaped like a key, creating a metaphoric connection to the topic of privacy and security (Figure 1). With this design, we aimed at achieving an interesting and engaging appearance that aids users in forming a mental model of its functionality. The *tangible*'s green *sensor state LEDs* are incorporated within their corresponding easily understandable *sensor icon* (representing presence, audio, and video sensing capabilities of smart home devices). Users can execute their privacy choices by pulling or pushing the *key teeth sliders*. The sliders clearly indicate their states since they cross the corresponding *sensor icon* out if the data collection is rejected. By combining these features, we created a distinct and intuitive connection between each *sensor icon*, its *state LED* and *key teeth slider*. The *PriKey-tangible* is 75 mm high, 40 mm wide and 17 mm deep. Our key-shaped object is easily reproducible, robust, compact, and lightweight, and provides intuitive means for tangible user input and immediate feedback.

4.2 PriKey-Station

The *PriKey-station* implements the awareness-increasing features of *PriKey*. Each room of a smart home has a *station* near the entrance door, where it can be easily seen by everybody entering the room. It lists all devices that are installed inside the room, their incorporated sensors (i.e., presence, video, or audio), and the sensor states. Moreover, it recognizes which devices and *tangible*s are inside the room and communicates with them (e.g., via Bluetooth or WiFi). The *station* can block the recording of individual sensors of smart devices (e.g., by jamming the audio signal). We envision the *PriKey-station* as a tablet-like device that permanently displays all nearby devices and integrated sensors (Fig. 1).

5 EXPLORATORY USER STUDY

In an exploratory user study, we investigated **RQ1 Perception of *PriKey*** and **RQ2 Privacy Considerations**.

5.1 Investigated Smart Home Scenarios

We investigated four scenarios, distinguishing *1) primary users*, *2) co-inhabitants*, *3) visitors in familiar environments* and *4) visitors in unfamiliar environments*. For both inhabitant scenarios (i.e., primary user and co-inhabitants), we asked participants to imagine living in a shared flat and the primary user just finished installing smart home devices in all rooms. The *visitor in a familiar environment* scenario involved visiting a friend in their smart home. For the *visitor in an unfamiliar environment* scenario, we asked participants to envision a rental apartment for a weekend trip.

Rooms. Each scenario comprised four rooms of a typical smart home: 1) *living room*, in which participants should imagine talking to a friend (e.g., over the phone); 2) going to the *bathroom* after finishing the conversation; 3) preparing and having dinner in the *kitchen* (together with their friend in the visitor in a familiar environment scenario); 4) reviewing photos of a (shared) memory on a laptop in the *bedroom*.

Smart Home Devices. Moreover, we incorporated a representative sample of smart home devices in the rooms. We chose the devices based on the previously mentioned top seller list from a leading online marketplace that we rated according to their *privacy intrusiveness*. Our rating is based on the idea that any additional sensor increases a device's privacy intrusiveness rather than directly comparing the privacy risks of different sensor types with each other. This approach allowed us to ensure that our scale is valid regardless of each sensor's particular risks. We distributed devices equally across the rooms, i.e., every room contains a device of each privacy intrusiveness level (see Table 1).

5.2 Apparatus

We provided all participants their own *PriKey-tangible*s, allowing tangible input and simulated feedback through LEDs. Moreover, we

Table 1: Rating of intrusiveness and device sample of the smart home simulation.

Sensors	Living Room	Bathroom	Kitchen	Bedroom
	Door Lock	Scale	Thermostat	Remote Control
	Smart Speaker	Decoration/ Light	Smart Speaker	Sleep Meter
	Security Camera	Smart Display	Security Camera	Smart Display

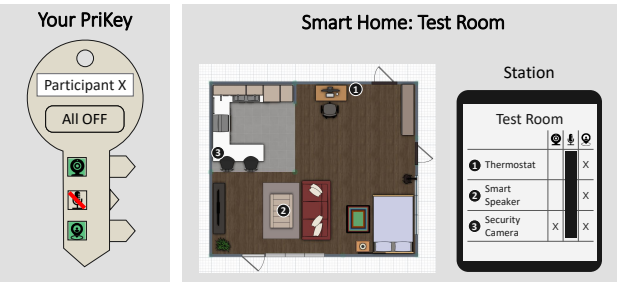


Figure 2: The smart home simulation click-prototype. The experimenter can visualize the corresponding effects of participants' privacy choices on the *tangible* and *station*.

developed a smart home simulation *click-prototype* to provide a consistent smart home setup for participants, including *PriKey-station*s for each room. We implemented the simulation using animations in Microsoft Power Point. Each slide included a click-sensitive visualization of the *tangible*, a visual representation of the current room and the corresponding *station* (Figure 2). Please note that the click-prototype was only used by the experimenter to adjust the simulation according to participants' interaction with their physical tangible such that they could observe the resulting effects on both, the *tangible* and the *station*.

5.3 Study Procedure

We conducted the study remotely using the video-conferencing tool Zoom. We sent *PriKey-tangible*s to participants via postal mail before the actual session. A session consisted of four phases[1]:

I. *Introductory Presentation.* After welcoming the participants and asking for their consent, our study started with an introductory presentation. This allowed us to evaluate participants' prior expertise on smart homes and ensure that all had a similar level of knowledge afterward.
II. *PriKey Trial.* Next, participants explored *PriKey*. We encouraged them to interact with our physical prototype and guided them through its functionality. We asked participants to think aloud and to answer questions on their opinions regarding both, the *PriKey-tangible* and the *station*. To reduce potential response biases, we did not mention that we developed *PriKey* and highlighted that we are searching for critical early feedback.
III. *Smart Home Simulation.* In this step, we introduced two scenarios (cf. Section 5.1). We randomly assigned participants to be either *visitor* or *inhabitant*, to let them conduct either both inhabitant scenarios (i.e., primary user and co-inhabitant) or visitor scenarios (i.e., in familiar and unfamiliar environments) in counterbalanced order, respectively. To create a consistent storyline, we did not counterbalance the order of the tasks (rooms).
IV. *Final Questionnaire & Interview.* We asked participants to fill in a questionnaire on the usability of *PriKey*, including the system usability scale (SUS) [7], the raw NASA task load index (RTLX) [23, 26, 28] and the human-computer trust scale (HCTS) [24]. Next, we conducted a semi-structured interview on their opinions regarding *PriKey* and the design of both, *tangible* and *station*. In this context, we inquired whether participants would prefer a smartphone app or the *PriKey-tangible*. Finally, participants provided demographics, including the internet users' information privacy concerns (IUIPC) [37] questionnaire.

[1]The fully study guide is available in the supplementary material of this paper.

5.4 Participants, Recruitment & Data Analysis

We recruited 16 participants by direct recruitment, social media posts, and through a University mailing list. All participants received a *PriKey-tangible* by postal mail. Sessions lasted between 60 and 90 minutes and were audio and video recorded. Participants were compensated through a 15€ voucher or study credits.

5.4.1 Ethical Considerations. Complying with legal requirements and our institutional ethics committees' guidelines, participants were first provided with detailed information on which data would be stored, how data storage was handled and that their participation was voluntary and could be aborted any time. At the beginning of a study session, all participants gave verbal consent to participate, which was video- and audio-recorded and stored independently. All other data was anonymized by transcribing audio recordings and applying anonymous identifiers. Note that, based on institutional guidelines and local laws, such low-risk user studies are exempt from formal approval by an IRB. However, we used checklists provided by our ethics committees to validate our study design in regards to ethical considerations.

5.4.2 Data Analysis. The transcribed interviews were analyzed using thematic analysis [6]. Two researchers independently familiarized themselves with the transcripts and conducted open coding to identify relevant themes and codes. One researcher considered all transcripts, and the other researcher half of the transcripts. Afterward, the two researchers met to discuss and organize the codes into a codebook, which was used for the final round of coding (cf. Supplementary Material B.5). If questions arose or new codes came up, the researchers met again to discuss any ambiguities. Due to the qualitative and exploratory nature of our study, we deliberately refrain from reporting measures of inter-rater agreement [42]. Differences in the coding process were solved through discussion.

5.4.3 Participants. Participants were 20 to 66 years old ($mean$ = 33.2, sd = 17.2). Eight participants identified as male and eight as female. Most participants were University students (N = 11). Six participants were living with their parents and siblings. Four

participants lived with their partner and children, three lived alone, and three lived in a shared flat (cf. Supplementary Material B.4). Seven participants owned or previously owned a smart home device, and eleven participants reported having used such devices before. Five participants never used a smart home device before. However, all participants could explain characteristics of a "smart home".

According to the IUIPC [37], most participants find it important to have *control* over their privacy online ($range$: 4.33 − 7.00, $mean$ = 6.19, sd = 0.74, $median$ = 6.17). Moreover, they are concerned by online companies *collecting* their data ($range$: 3.67−7.00, $mean$ = 6.29, sd = 1.02, $median$ = 6.67). Lastly, some find features informing on privacy invasions important while others are less concerned (*awareness*, $range$: 2.00 − 7.00, $mean$ = 5.61, sd = 1.69, $median$ = 6.38). From the interviews, we found that most participants were *concerned* about their privacy in smart homes (N = 13). Eight participants mentioned feeling *observed* by devices. Four participants reported feeling uninformed regarding possible privacy intrusions by such technology. Also, participants were concerned about *unauthorized parties* accessing sensitive data (N = 4) and expressed *mistrust* in device providers (N = 4). Some participants stated to not have purchased such technology in the past or removed already installed devices due to related concerns (N = 6).

5.5 Limitations

Similar to all studies that rely on self-reported data, our investigation may be subject to the social desirability bias, availability bias, and potential wrong self-assessments. Moreover, the composition of our sample is biased towards young (mean age 33.2 years) students. Hence, our insights might not apply to the general public, but participants represent early adopters of technology. With our study, we collect first feedback on *PriKey*. Based on that, the participants interacted with our prototype only once. Long-term usage of *PriKey* has to be investigated by future studies. Moreover, to render our concept comprehensible for the participants, we based the user study on our Wizard-of-Oz implementation of *PriKey*. However, the *PriKey* concept is much more extensive and needs further in-depth investigations.

6 RESULTS

Our exploratory user study provides a hands-on evaluation of *users' perceptions regarding tangible privacy mechanisms for smart homes* as well as answering open questions on *users' corresponding privacy considerations*. Participants conducted scenarios around being inhabitants (P_i) or visitors (P_v).

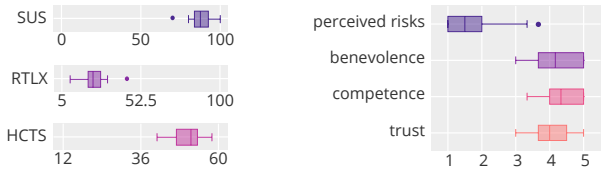
6.1 RQ1.1 Interaction with PriKey

We now present participants' perception towards our prototype and concept, as well as their interaction with *PriKey*.

6.1.1 *Quantitative Results.*

Perceived Usability. *PriKey*'s usability was rated *excellent* [5] with a SUS score [7] of 87.66 (sd = 7.72, $median$ = 87.5). The workload caused by *PriKey* received an average RTLX score [23, 26, 28] of 24.17 (sd = 8.04, $median$ = 23.75), which is *very low* [23].

Trust. We computed the HCTS score [24] by inverting the answers of negative statements and summing all 12 values [3, 4].



(a) SUS, RTLX and HCTS **(b) HCTS subscale scores**

Figure 3: Boxplots of *PriKey*'s SUS, RTLX and HCTS scores.

Hence, HCTS scores can range from 12 (low trust) to 60 (high trust). Our participants evaluated the trust inspired by *PriKey* on average with a score of 50.29 (sd = 5.09, $median$ = 52, see Figure 3a). We also calculated participants' average scores for each HCTS subscale (can range from 1 (low) to 5 (high), see Figure 3b). The *perceived risk* of using *PriKey* was rated with 1.77 (sd = 1.02, $median$ = 1) and our system's *benevolence* with 4.18 (sd = 0.96, $median$ = 4). Furthermore, participants rated the *competence* of *PriKey* on average with 4.42 (sd = 0.79, $median$ = 5) and their *trust* in our system with 4.06 (sd = 0.84, $median$ = 4).

6.1.2 *Feedback on the Concept.*

Participants liked our system as it enables intuitive (N = 5) and fast (N = 3) interactions. However, many participants also expected to be able to exert control on each device independently rather than only by sensor groups (N = 8). Nevertheless, participants felt that *PriKey* increases awareness of possible privacy intrusions (N = 7) and specifically empowers visitors to execute personal privacy choices (N = 8):

"(...) even if the person (...) informs me about it, there is bound to be something – even without intention – that gets forgotten (...). And I find it very pleasant when I can simply take care of it myself." ($P2_i$)

Moreover, some participants positively emphasized that *PriKey* already enables configuring privacy choices proactively, i.e., even before being exposed to the actual situation (N = 3). Nevertheless, some participants highlighted that our system could cause conflicts between the interests of different stakeholders (i.e., primary user and visitor, N = 6). Two participants would consider a smart devices' purpose before using *PriKey* to deactivate data collection and/or first inform the primary user (here: a friend): *"I would talk to [my friend] and indicate that I do not want to be recorded."* ($P14_i$) Some participants also discussed possible threats for their privacy imposed through *PriKey* (N = 4), mentioning that it needs to collect sensitive data (e.g., users' presence) to operate correctly and that attackers could gain physical access to the *PriKey-tangible* and disable *PriKey*. Furthermore, participants expressed mistrust in *PriKey* since they must always rely on its correct functioning to protect their privacy (N = 5): *"(...) it is also a matter of trust whether what I configure there actually happens. (...)"* ($P16_v$)

6.1.3 *Feedback on the Prototype.*

We discuss participants' feedback on our prototype: the *tangible* and the *station*.

Tangible. Most participants intuitively knew how to use the *PriKey-tangible* to execute their privacy choices (N = 12). Some also stated that the *tangible* is handy (N = 3) and has a good size (N = 2). The *All off* button was considered convenient by three participants and, thus, used to deactivate all data collection. Many participants

found the key shape of our *tangible* fun or interesting ($N = 9$). The underlying metaphor was perceived positively ($N = 5$):

"(...) it symbolizes privacy because [it is] the key, so to speak, to your own privacy. And you can then decide for yourself (...)." ($P4_v$)

However, $P2_i$ and $P3_v$ would prefer a simpler design inspired by classical remote controls. Some participants further mentioned that the *tangible* should be smaller ($N = 6$) and thinner ($N = 3$). Moreover, they commented that the *PriKey-tangible* looks like a prototype ($N = 4$) and fragile ($N = 5$).

Most participants appreciated the sensor state LEDs, since they provide valuable feedback ($N = 14$) and intuitively knew how to use the key teeth sliders to configure their privacy choices ($N = 14$). However, some participants would prefer common buttons instead of sliders ($N = 4$). Moreover, all 16 participants assessed the functionality of the *all off* button correctly, and four specifically mentioned that it is convenient.

Station. When we asked our participants on the *PriKey-station*, most indicated that its design was intuitive ($N = 9$). Some participants suggested visualizing the states of the sensor groups differently ($N = 6$), e.g., by placing the icons of incorporated sensors next to each device name instead of visualizing a table ($P6_i$), using colors ($N = 3$) or blurring out deactivated sensor groups ($P1_i$). Moreover, some wished the *station* to differ from a normal tablet ($N = 2$) and that it should be implemented using smaller displays ($N = 2$):

"A small display is actually sufficient, maybe not necessarily a tablet that is bigger." ($P2_i$)

6.1.4 Comparison to Smartphone App. Eight participants would prefer a smartphone app with capabilities similar to *PriKey*, because they would not need an extra device (i.e., the *tangible*, $N = 6$), and they usually have their smartphone close by anyway ($N = 3$):

"(...) I always have my smartphone with me anyway - my bag is always full, so the less I have to carry, the better." ($P14_i$)

However, five participants would prefer *PriKey*, since the *tangible* is more ready-to-hand and direct ($N = 4$):

"(...) I would prefer PriKey because it's so easy to use and with the smartphone, I would have to swipe around a bit and then look for the app and then it could be that the battery is empty (...)." ($P10_i$)

Some participants also stated to trust *PriKey* more than a smartphone app ($N = 2$):

"(...) it seems very much as if no one could tinker with your system. It seems very external." ($P9_i$)

Furthermore, $P6_i$ explained that having the *tangible* serves as a reminder to think about privacy. The remaining three participants stated that they would try both *PriKey* and the app for some time and afterward decide which one they would like to continue using.

6.2 RQ1.2 Broader Implications of *PriKey*

We present participants' opinions on who should be responsible for providing users with *PriKey-tangible*s and their visions for future implementations and use cases of *PriKey*.

6.2.1 Role-Dependent Adoption and Responsibility. Most participants would use *PriKey* as a visitor ($N = 15$), but also in their own home ($N = 13$), especially if it was shared ($P7_v$). Participants who would not use *PriKey* at their own home ($N = 4$) stated that no one else would be able to access their devices anyway or that they would configure their own devices to minimize privacy risks.

Furthermore, we asked participants who should be *responsible for providing users with a PriKey-tangible*. Most stated that everybody would be responsible for getting their personal *tangible* ($N = 14$). Three participants highlighted that primary users should, nevertheless, transparently disclose possible privacy intrusions. Only two participants felt that anyone entering a smart environment should be provided with a *PriKey-tangible* by the primary smart devices user. Some stated that primary users should generally provide visitors with *tangible*s, but they would nevertheless buy one themselves to make sure they really have one when needed ($N = 3$).

6.2.2 Future Implementations. Participants mentioned how they envision future implementations of *PriKey*. $P3_v$ and $P8_v$ suggested combining *tangible* and *station*, e.g., by incorporating a screen in the tangible ($P3_v$) or including control functionalities in the station ($P8_v$). Similarly, $P16_v$ envisioned a *PriKey-station* that also serves as a smart display (e.g., visualizing general data like time and temperature). $P8_v$ and $P4_v$ suggested using the *PriKey-tangible* as a personal authentication token. Hence, an individual's level of access could be stored on the *PriKey-tangible* (e.g., whether this person is allowed to configure a smart home device). $P8_v$ envisioned the *PriKey-tangible* as a token to unlock a rental apartment's smart door lock and could imagine incorporating a fingerprint sensor in our *tangible* so that it can only be used by its owner. $P11_v$ suggested using metal instead of plastics for the *PriKey-tangible*.

6.2.3 Further Use Cases. Participants stated that they would use *PriKey* to protect their privacy in various environments ($N = 10$). For instance, participants mentioned public spaces ($N = 7$, e.g., restaurants or malls), hotels ($N = 4$), visits of unfamiliar households ($N = 3$), workplaces ($N = 3$), doctor's offices ($N = 2$) and "everywhere" ($N = 4$). However, participants also mentioned that for some sensors, not everybody should have the power to control them ($N = 7$, e.g., security cameras of restaurants or shops). $P4_v$ suggested rather raising awareness of intrusions in public spaces. Some participants also envisioned using *PriKey* in the future when sophisticated smart home setups would be more common ($N = 6$). Furthermore, $P7_v$ imagined that older adults could benefit from the intuitive handling of our *tangible*. $P9_i$ felt that *PriKey* should be made available especially to persons who are exposed to particular security risks due to their profession (e.g., teachers, government employees).

6.3 RQ2 Privacy Considerations

We report participants' *privacy considerations* while using *PriKey* as well as their various *choices*.

6.3.1 Privacy Considerations. Most participants agreed that providing everybody with the means to protect their own privacy is important ($N = 14$). Participants *accepted the collection of data* from certain sensor types to use a certain smart home device and its functionalities ($N = 9$ participants). Many participants were not concerned by the data collection ($N = 9$) or accepted it due to convenience ($N = 3$). Few participants also stated that the data would be shared anyway ($N = 3$). If participants *denied the data collection*, they usually wanted to protect their privacy ($N = 15$) or reasoned

that they do not need some devices in a specific scenario ($N = 7$). Hence, participants' general privacy considerations were consistent with findings from related works [1, 41, 64]. However, they also expressed specific considerations that we grouped by topics:

Sensor Dependency. Most participants were specifically concerned about video ($N = 12$) and audio recordings ($N = 8$), which is consistent with prior work [12, 62, 63]. Four participants specifically mentioned generally accepting presence sensing capabilities of smart home devices.

Device Dependency. Similar to prior work [1, 12, 39, 62], participants frequently based their privacy decisions on the affected smart home devices. Most participants asked about the utility of a device ($N = 10$) or inquired whether a specific device would still provide basic capabilities (e.g., light, $N = 8$) before taking a decision. We also observed that some were especially concerned about smart speakers ($N = 6$): *"(...) if there is an Alexa in the room, I would like the Alexa to be completely off. Alexa should not even know that I am in the room."* ($P8_v$)

Role Dependency. Participants also based privacy decisions on their role and their relation to the primary user. In line with related work [41], participants highlighted that the trust in the primary user would be decisive ($N = 8$). Participants also assumed that only the primary user was able to access the collected data ($N = 6$) and is most interested in the device being fully functional ($N = 2$). Some participants further argued that primary users already inherently consented to data collection when purchasing the devices ($N = 3$), which corresponds to findings from related work [25].

Room/Task Dependency. We observed an influence of the different rooms or tasks of our smart home simulation. Most participants explained that they would not want to be exposed to video ($N = 11$) or audio sensing ($N = 4$) in the *bathroom*, since it was perceived as an intimate environment ($N = 5$). Participants reported similar concerns regarding video cameras ($N = 2$) in the *bedroom*, because this room also represented an intimate environment ($N = 4$). Some participants mentioned not wanting to have co-inhabitants' devices in their bedroom ($N = 2$). These findings are consistent with observations in related work [39]. Moreover, participants considered the *bedroom* task before taking their privacy choices ($N = 6$) and some thought about protecting the photos from installed cameras ($N = 3$). They also wanted to prevent smart home devices from overhearing their conversation ($N = 10$) in the *living room* task. However, the tasks in the *kitchen* (i.e., preparing dinner and eating) were perceived as not sensitive ($N = 6$).

6.3.2 Quantitative Privacy Choices. On average, each participant deactivated sensors with *PriKey* 10.88 times ($sd = 6.25$, $range : 0 - 22$). Table 2 lists the conditions under which participants disabled data collection of each sensor group. Participants opted for deactivating sensors in 46.88% of the 384 possible occasions. Video cameras were the most frequently deactivated (60.16% of 128 deactivations), followed by audio (47.66%) and presence sensing (32.81%).

Rooms/Tasks. We found that participants turned off sensors most frequently in the bathroom (62.50% of 96 occasions), followed by the living room (58.33%), bedroom (39.58%) and kitchen (27.08%).

Roles. Visitors in unfamiliar environments deactivated sensors most frequently (64.58% of 96 possible occasions), followed by visitors in familiar environments (56.25%), co-inhabitants (37.50%), and primary users (29.17%). Hence, deactivations decreased with increasing level of familiarity.

6.4 Summary

Addressing **RQ1 Perception of *PriKey***, we gathered quantitative and qualitative feedback. We evaluated participants' perception of their interaction with *PriKey* (**RQ1.1**). *PriKey* was rated with excellent usability, low workload, and generally trustworthy. Participants appreciated many features (e.g., its intuitiveness, $N = 5$ and proactive privacy control, $N = 3$) of *PriKey*, but missed the ability to control devices independently ($N = 8$). Moreover, they mentioned a potential for conflicts between different stakeholders ($N = 6$) and threats to their privacy ($N = 4$) imposed by *PriKey*. Regarding our implementation, most participants intuitively knew how to configure their privacy choices using the *PriKey-tangible* ($N = 14$) and liked its key shape ($N = 9$).

For **RQ1.2**, most participants of our study would use *PriKey* to protect their privacy, especially when visiting a smart home ($N = 15$) and be responsible themselves for holding their own *PriKey-tangible* ($N = 14$). Participants envisioned future combinations of *tangible* and *station* ($N = 3$) and adding authentication functionalities to the *tangible* ($N = 2$).

Regarding **RQ2 Privacy Considerations**, we found that our participants' *PriKey* specific privacy considerations varied largely depending on personal factors, like their roles, the executed task or current surrounding, and their individual risk perceptions regarding specific sensors or devices. This resulted in an observable decrease in the usage of *PriKey* in relation with: (a) the users' familiarity with the environment, (b) the perceived intimacy of the current context (i.e., room or task) and (c) the incorporated sensors.

7 COMPARISON USER STUDY

To answer **RQ3 - Comparison**, we conducted a second study comparing *PriKey* to an equivalent mobile app, referred to as *PriPhone*. We chose this comparison as we considered an app being state-of-the-art for smart home privacy mechanisms [18, 29]. We did not compare *PriKey* to existing smartphone privacy control apps, since these are frequently manufacturer specific and provide very different control and awareness functionalities, which would result in uncontrolled confounding effects for our evaluation. Hence, we developed a smartphone app click-prototype with capabilities that closely correspond to *PriKey*'s features. Moreover, we specifically focused on visitors in unfamiliar smart homes, as this was the most prominent use case in our first exploration.

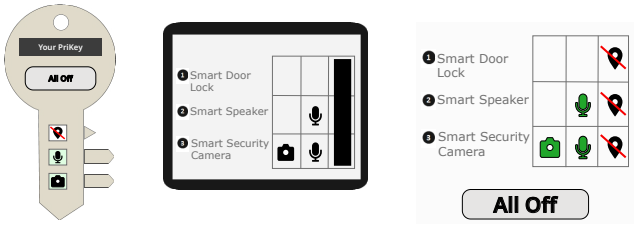
7.1 Study Methodology

In this study, participants were presented with two prototypes of smart home privacy mechanisms with identical functionality: *PriKey*, a *tangible* mechanism as previously described; and *PriPhone*, conceptualized as a smartphone app.

7.1.1 Apparatus: Clickable Prototypes. We prepared two clickable prototypes to guide participants through a simulated smart home environment, one for *PriKey* and one for *PriPhone* (see Figure 4).

Table 2: Sensor deactivations per room and per role. Overall, 180 sensors were deactivated (presence: 42, audio: 61, video: 77).

room	presence	audio	video	all sensors	role	presence	audio	video	all sensors
living room	12	22	22	56	primary user	4	11	13	28
bathroom	15	20	25	60	co-inhabitant	5	13	18	36
kitchen	7	6	13	26	visitor familiar	14	17	23	54
bedroom	8	13	17	38	visitor unfamiliar	19	20	23	62



(a) PriKey **(b) PriPhone**

Figure 4: Click-Prototypes for *PriKey* (a) and *PriPhone* (b). Both were shown next to a floor plan (similar to Figure 2).

The prototypes were implemented using Adobe XD and included all rooms and devices from our exploratory study (see Section 5.2). *PriPhone* is conceptualized as a smartphone app with an identical functionality as *PriKey*. Clicking on sensor icons or the *All Off* button turns off the respective sensors of all devices in the room.

7.1.2 Study Procedure. We introduced participants to the topic of smart home privacy and guided them through the *visitor in an unfamiliar environment* scenario for each mechanism separately. For every mechanism, we asked them to fill in the SUS [7], RTLX [27, 28]) and HCTS [24]. In this study, we additionally added the UEQ to assess user experience [35]. We counterbalanced the order of the mechanisms and visualized rooms. After participants had experienced both mechanisms, we asked them to compare them in a final questionnaire (cf. Supplementary Material C.1). We collected participants' demographics, technical affinity [19] and the IUIPC [37]).

7.1.3 Recruitment & Gathered Data. We recruited 32 new participants directly and through a University mailing list. The study was conducted through a video call. A session lasted 60 minutes and was audio- and video-recorded. Participants were compensated with 10€ vouchers or study points.

7.1.4 Ethical Considerations. This user study complied with legal requirements and institutional guidelines, equivalent to the exploratory study (cf. Section 5.4.1 for more details).

7.1.5 Participants. Participants were between 18 and 32 years old. Most participants ($N = 17$) fell in the range between 23 and 27 years, with six being younger and nine being older. 21 participants identified as male and eleven as female. Most participants were students ($N = 25$), and more than half of them owned a smart home device ($N = 18$). According to the IUIPC [37], participants' wish for *control* ranged from 2.67 to 7.00 ($mean = 6.04$, $sd = 0.92$, $median = 6.17$), perceived data *collection* from 3.50 to 7.00 ($mean = 5.84$, $sd = 0.92$, $median = 6.00$) and *awareness* ranged from 4.33 to 7.00 ($mean = 6.31$, $sd = 0.71$, $median = 6.50$). Participants' ATI [19] ranged from 2.78 to 6.00 ($mean = 4.67$, $sd = 0.79$, $median = 4.61$).

7.1.6 Limitations. Limitations of this study are in line with the prototype exploration (cf. Section 5.5). In addition, participants in this study did not directly interact with the *PriKey-tangible* prototype, which might have influenced their perception. However, we believe this impact to be minimal as online studies are an effective tool in HCI research [60].

7.2 Results

To identify statistically significant differences between both mechanisms, we used undirected paired samples t-tests. If the normality assumption, as indicated by Shapiro-Wilk's test, was violated, a Wilcoxon test was employed instead. Moreover, one researcher collected aspects from the questionnaires' free-text answers and identified common themes.

7.2.1 User Experience. *PriPhone* received higher UEQ scores than *PriKey* for attractiveness, dependability, efficency, perspicuity and stimulation [52] (see Table 3). Only the novelty was rated higher for *PriKey*. While attractiveness ($t(31) = -2.61, p < 0.05, d = -0.46$), efficiency ($W = 84.50, p < 0.05, r = -0.52$) and novelty ($t(31) = 2.73, p = 0.01, d = 0.48$) showed significant differences for both mechanisms, dependability, perspicuity and stimulation did not ($p >= 0.16$).

7.2.2 Perceived Usability. *PriKey* received a mean SUS score of 79.80 ($median = 80.00$, $sd = 13.48$) and *PriPhone* of 88.20 ($median = 90.00$, $sd = 7.60$, see Figure 5). A Wilcoxon test revealed significant differences between both ($W = 46.00, p < .001, r = -0.79$). *PriKey* received a mean RTLX score of 20.70 ($median = 21.30$, $sd = 11.10$) and *PriPhone* of 18.40 ($median = 18.30, sd = 10.40$). We found significant differences between both samples ($t(31) = 2.02, p = 0.05, d = 0.36$).

7.2.3 Trust. We calculated the HCTS scores as described in Section 6.1.2). *PriKey* received a mean score of 42.00 ($median = 41.50$, $sd = 8.34$) and *PriPhone* of 42.60 ($median = 43.00, sd = 8.32$). Further analysis showed no significant differences ($t(31) = -0.66, p =$

Table 3: UEQ descriptives for *PriKey* and *PriPhone* sample. Higher mean scores were highlighted using bold font.

	PriKey			PriPhone		
subscale	mean	median	std	mean	median	std
attractiveness	1.33	1.17	1.01	**1.63**	1.63	0.87
dependability	1.56	1.63	0.83	**1.60**	1.50	0.8
efficency	1.60	1.75	0.97	**1.97**	2.00	0.73
novelty	**1.34**	1.50	1.09	0.78	0.75	1.07
perspicuity	2.24	2.50	0.85	**2.48**	2.75	0.66
stimulation	0.97	0.75	0.93	**1.18**	1.38	0.92

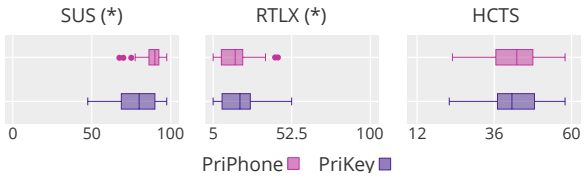


Figure 5: SUS, RTLX and HCTS scores for *PriKey* and *PriPhone*. (*) denotes statistically significant differences.

Table 4: Results of HCTS subscales for *PriKey* and *PriPhone*. Higher mean scores were highlighted using bold font.

	PriKey			PriPhone		
subscale	mean	median	std	mean	median	std
perceived risk	**2.20**	4.00	0.96	2.01	4.00	0.90
benevolence	**3.73**	3.67	0.73	3.47	3.33	0.88
competence	3.39	3.33	0.95	**3.54**	3.67	0.95
trust	3.09	3.17	0.89	**3.21**	3.33	0.97

0.51). Descriptives for each subscale can be found in Table 4. The perceived risks of using *PriKey* were rated higher than *PriPhone*. Correspondingly, our participants rated the competence and trust of *PriKey* lower compared to *PriPhone*. The benevolence of *PriKey* received a higher rating than *PriPhone* (non-significant, $p >= 0.08$).

7.2.4 Perception of Both Mechanisms. When asked which mechanism is overall preferred, 24 participants chose *PriPhone*. 20 of them stated that *PriKey* would be like another remote control. They disliked having to carry it around, were worried they might forget or break it, or were already used to smartphone apps. Eight participants overall preferred *PriKey*. Some participants mentioned concerns with *PriPhone*, since it requires the installation of an app ($N = 6$) and likely collects more user data ($N = 1$). Four participants found *PriKey* more interesting, exciting, and fun to use. One participant felt more encouraged to actively use *PriKey* compared to the app, another appreciated *PriKey* for visitors. Some (*PriPhone*: 7, *PriKey*: 5) participants additionally mentioned that they would like to have the possibility to deactivate sensors for each smart home device independently.

8 DISCUSSION & FUTURE RESEARCH

The *PriKey* concept constitutes a first approach on *device independent, sensor based, user centric, and power-equalizing tangible smart home privacy mechanism*. We discuss open questions for future research below.

8.1 Tangible Privacy Mechanisms

Some participants of both our user studies favored *PriKey* over a similar smartphone app. Moreover, most participants of the exploratory study intuitively knew how to interact with the *PriKey-tangible*. The *PriKey* prototype was also perceived as more fun, engaging, encouraging, and benevolent compared to the app by participants of both studies. These findings indicate that the concept of tangible privacy mechanisms is indeed a noteworthy approach for future developers and researchers alike. We discuss further opportunities of the concept below.

8.1.1 Multi-Modal and Hybrid Mechanisms. Based on users' diverging preferences observed in our study and in related work [1, 46, 61], we argue that future smart home privacy mechanisms should enable users to choose their preferred interaction modality, rather than trying to fit one approach to all individuals. We, thus, believe that respecting individuals' interaction preferences by-design is key to developing truly usable, engaging and trusted privacy enhancing technologies. Hence, our findings inspire the development of *mechanisms that are compatible with multiple in- and output gadgets*, which allow users to ultimately *decide for themselves* whether they prefer a tangible or a non-tangible device. Based on participants' suggestions, we also envision *hybrid systems that incorporate tangible control functionalities while also enabling more detailed non-tangible awareness features.*

8.1.2 Form Factor. Most participants appreciated the *tangible*'s key shape and the underlying security-related metaphor, while others suggested a simpler form-factor. Hence, we see potential for *future in-depth research on the effects of differently shaped privacy mechanisms on users' behavior or cognitive processes* (e.g., perceived trust, long-term usage, cognitive load, metal models). Moreover, since personal fabrication technology, like 3D printers, has become increasingly accessible [48], *we envision a future where users can easily customize the shape of their tangible privacy mechanism.*

8.1.3 Alternative Comparisons. In our second study, we compared *PriKey* to a smartphone app. Most participants of both studies would prefer a smartphone app over *PriKey*, because they would not need another device and always have their smartphone nearby anyways. Hence, they did not object to tangible interactions in general, but to having to carry around more hardware. Moreover, *familiarity* and *novelty bias* could have influenced participants perceptions, since they all used their smartphone on a regular basis. We, thus, suggest *comparing tangible privacy controls for smart homes with equally novel non-tangible mechanisms*, such as touchscreen-based privacy controls.

8.2 Smart Home Privacy Controls

We were also able to gain insights on open questions for general research on smart home privacy mechanisms.

8.2.1 Social Aspects and Conflicts. Participants in our prototype exploration suggested that individuals should be *responsible* for having their *own PriKey*, rather than primary users providing it to visitors. This would empower visitors to act according to their privacy needs in arbitrary environments. At the same time, participants raised a potential for conflicts and visitors might hesitate to actually use their *PriKey*. Hence, future research should investigate *conflict mitigation between various individuals* (i.e., between multiple primary users or visitors, between primary users and visitors and between individuals in other hierarchical relationships, like children and parents), e.g., by means of *cooperative control mechanisms* [62]. Furthermore, our participants also suggested using *PriKey* in public spaces, which results in open research questions regarding conflicts between different stakeholders. Hence, further research on, e.g., *focusing on raising awareness rather than providing control as potentially acceptable trade-off for public contexts* is necessary.

8.2.2 Sensor-Based Grouping and User-Centric Range. Our findings and related work [9, 64] suggest that users' privacy concerns are sensor-dependent. For instance, participants deactivated video and audio recordings particularly frequently and were also most concerned about such footage. We, thus, argue that *PriKey*'s *sensor-based grouping of privacy choices supports users well, while reducing complexity*. However, participants of both studies also expected to be able to execute privacy decisions independently for each smart home device. Therefore, we see a need for further research on *possible combinations of user-centric sensor-based privacy choices and control features for individual smart home devices*. Moreover, to reduce complexity, *PriKey* applied a simplified definition of user-centric range by applying privacy choices to all devices inside the same room, as we considered these most privacy relevant. Hence, *future research is necessary to evaluate whether devices outside the current room might still impose privacy risks and how these could be mitigated*. For example, a combination of a user-centric approach with a fixed distance (e.g., affecting all devices that are less then 10 meters away from the user) and our current room-based approach *PriKey* could be investigated.

8.2.3 Threats. A smart home privacy mechanism usually constitutes an additional sensor-enhanced and connected device and, as such, comes with new risks for users' privacy and security. As observed by one participant, the *PriKey-station* needs to detect the presence of a user to enable control over devices in that room. Hence, *the extent of privacy and security risks imposed by such privacy mechanisms should be further investigated in future research.* As suggested by $P8_{\mathcal{U}}$, the mechanism could further *provide authentication features like a fingerprint sensor*. This would allow mitigating risks imposed by the unauthorized access of a third party that could, e.g., disable *PriKey*'s privacy protection.

9 CONCLUSION

In this paper, we present *PriKey*, a concept for uncomplex, device-independent and power-equalizing tangible privacy mechanisms for smart homes, along with an implementation sample. We investigated users' perceptions of our concept in two user studies, one in comparison with a smartphone app. While many users tended towards preferring the app, we found that they also appreciated the intuitive, encouraging, engaging, and direct interactions that *PriKey* facilitates. Moreover, in line with related work, users' adoption of *PriKey* was influenced by personal factors, such as their roles, individual risk perceptions, or current context (i.e., intimacy and familiarity of the environment or installed devices). We derive open questions for the design of (tangible) smart home privacy mechanisms. Our work can serve as a stepping stone for future research on privacy mechanisms, also beyond smart homes.

ACKNOWLEDGMENTS

We would like to thank all our study participants for their time and valuable feedback on our concept. This project has been funded by the German Federal Ministry of Education and Research (BMBF) within the SWC 2.0 "PrivacyGate" 01|S17050, by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr [MuQuaNet] and by the German Research Foundation (DFG) under project no. 425869382.

REFERENCES

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

[2] Shimaa Ahmed, Ilia Shumailov, Nicolas Papernot, and Kassem Fawaz. 2022. Towards More Robust Keyword Spotting for Voice Assistants. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA. https://www.usenix.org/conference/usenixsecurity22/presentation/ahmed

[3] Ighoyota Ben Ajenaghughrure, Sonia Claudia da Costa Sousa, and David Lamas. 2020. Risk and Trust in artificial intelligence technologies: A case study of Autonomous Vehicles. In *2020 13th International Conference on Human System Interaction (HSI)*. IEEE, 118–123.

[4] Ighoyota Ben Ajenaghughrure, Sonia Cláudia Da Costa Sousa, and David Lamas. 2021. Psychophysiological Modeling of Trust In Technology: Influence of Feature Selection Methods. *Proc. ACM Hum.-Comput. Interact.* 5, EICS, Article 203, 25 pages. https://doi.org/10.1145/3459745

[5] Aaron Bangor, Philip Kortum, and James Miller. 2009. Determining what individual SUS scores mean: Adding an adjective rating scale. *Journal of usability studies* 4, 3 (2009), 114–123.

[6] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. https://doi.org/10.1191/1478088706qp063oa

[7] John Brooke. 1996. *SUS – a quick and dirty usability scale.* Taylor & Francis, 189–194.

[8] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. 2016. On Privacy and Security Challenges in Smart Connected Homes. In *2016 European Intelligence and Security Informatics Conference (EISIC)*. 172–175. https://doi.org/10.1109/EISIC.2016.044

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

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

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

[12] Camille Cobb, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer. 2021. "I would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. *Proceedings on Privacy Enhancing Technologies* 2021, 4 (2021), 54–75.

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

[14] Anupam Das, Martin Degeling, Daniel Smullen, and Norman Sadeh. 2018. Personalized Privacy Assistants for the Internet of Things: Providing Users with Notice and Choice. *IEEE Pervasive Computing* 17, 3 (Jul 2018), 35–46. https://doi.org/10.1109/MPRV.2018.03367733

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

[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. https://doi.org/10.1145/3494983

[17] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proc. of the CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. ACM, New York, NY, USA, Article 534, 12 pages. https://doi.org/10.1145/3290605.3300764

[18] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things.

In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 64, 16 pages. https://doi.org/10.1145/3411764.3445148

[19] 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.

[20] Batya Friedman, David Hurley, Daniel C. Howe, Edward Felten, and Helen Nissenbaum. 2002. Users' Conceptions of Web Security: A Comparative Study. In *CHI '02 Extended Abstracts on Human Factors in Computing Systems* (Minneapolis, Minnesota, USA) *(CHI EA '02)*. Association for Computing Machinery, New York, NY, USA, 746–747. https://doi.org/10.1145/506443.506577

[21] Radhika Garg and Christopher Moreno. 2019. Understanding Motivators, Constraints, and Practices of Sharing Internet of Things. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 3, 2, Article 44 (June 2019), 21 pages. https://doi.org/10.1145/3328915

[22] 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. https://doi.org/10.1145/3290605.3300498

[23] Rebecca Grier. 2015. How high is high? A metanalysis of NASA TLX global workload scores. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 59. https://doi.org/10.1177/1541931215591373

[24] Siddharth Gulati, Sonia Sousa, and David Lamas. 2019. Design, development and evaluation of a human-computer trust scale, journal = Behaviour & Information Technology. 38, 10 (2019), 1004–1015. https://doi.org/10.1080/0144929X.2019.1656779

[25] Julie Haney, Yasemin Acar, and Susanne Furman. 2021. "It's the Company, the Government, You and I": User Perceptions of Responsibility for Smart Home Privacy and Security. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 411–428. https://www.usenix.org/conference/usenixsecurity21/presentation/haney

[26] Sandra G Hart. 2006. NASA-task load index (NASA-TLX); 20 years later. In *Proceedings of the human factors and ergonomics society annual meeting*, Vol. 50. Sage publications Sage CA: Los Angeles, CA, 904–908.

[27] Sandra G. Hart. 2006. Nasa-Task Load Index (NASA-TLX); 20 Years Later. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 50, 9 (2006), 904–908. https://doi.org/10.1177/154193120605000909

[28] Sandra G. Hart and Lowell E. Staveland. 1988. Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research. In *Human Mental Workload*, Peter A. Hancock and Najmedin Meshkati (Eds.). Advances in Psychology, Vol. 52. North-Holland, 139–183. https://doi.org/10.1016/S0166-4115(08)62386-9

[29] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. 2018. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, Baltimore, MD, 255–272. https://www.usenix.org/conference/usenixsecurity18/presentation/he

[30] Yangyang He. 2019. Recommending privacy settings for IoT. In *Proceedings of the 24th International Conference on Intelligent User Interfaces Companion - IUI '19*. ACM Press, Marina del Ray, California, 157–158. https://doi.org/10.1145/3308557.3308732

[31] Almut Herzog and Nahid Shahmehri. 2007. User Help Techniques for Usable Security. In *Proceedings of the 2007 Symposium on Computer Human Interaction for the Management of Information Technology* (Cambridge, Massachusetts) *(CHIMIT '07)*. Association for Computing Machinery, New York, NY, USA, 11–es. https://doi.org/10.1145/1234772.1234787

[32] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "Nutrition Label" for Privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (Mountain View, California, USA) *(SOUPS '09)*. Association for Computing Machinery, New York, NY, USA, Article 4, 12 pages. https://doi.org/10.1145/1572532.1572538

[33] 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*. Association for Computing Machinery, New York, NY, USA, 149–159. https://doi.org/10.1145/3461778.3462073

[34] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-Seeking Behaviors With Smart Speakers. *Proc. of the ACM Conference on Human-Computer Interaction* 2, CSCW (2018), 102. https://doi.org/10.1145/3274371

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

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

[37] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355.

[38] Shrirang Mare, Logan Girvin, Franziska Roesner, and Tadayoshi Kohno. 2019. Consumer Smart Homes: Where We Are and Where We Need to Go. In *Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications* (Santa Cruz, CA, USA) *(HotMobile '19)*. Association for Computing Machinery, New York, NY, USA, 117–122. https://doi.org/10.1145/3301293.3302371

[39] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. *Proc. Priv. Enhancing Technol.* 2020, 2 (2020), 436–458.

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

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

[42] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. of the ACM on Human-Computer Interaction (HCI)* 3, CSCW, Article 72 (Nov. 2019), 23 pages. https://doi.org/10.1145/3359174

[43] Vikram Mehta. 2019. Tangible Interactions for Privacy Management *(TEI '19)*. Association for Computing Machinery, New York, NY, USA, 723–726. https://doi.org/10.1145/3294109.3302934

[44] Vikram Mehta, Arosha K. Bandara, Blaine A. Price, and Bashar Nuseibeh. 2016. Privacy Itch and Scratch: On Body Privacy Warnings and Controls. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 2417–2424. https://doi.org/10.1145/2851581.2892475

[45] Vikram Mehta, Arosha K. Bandara, Blaine A. Price, Bashar Nuseibeh, and Daniel Gooch. 2021. Up Close & Personal: Exploring User-Preferred Image Schemas for Intuitive Privacy Awareness and Control. In *Proceedings of the Fifteenth International Conference on Tangible, Embedded, and Embodied Interaction* (Salzburg, Austria) *(TEI '21)*. Association for Computing Machinery, New York, NY, USA, Article 7, 13 pages. https://doi.org/10.1145/3430524.3440626

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

[47] Richard Mitev, Anna Pazii, Markus Miettinen, William Enck, and Ahmad-Reza Sadeghi. 2020. LeakyPick: IoT Audio Spy Detector. In *Annual Computer Security Applications Conference* (Austin, USA) *(ACSAC '20)*. Association for Computing Machinery, New York, NY, USA, 694–705. https://doi.org/10.1145/3427228.3427277

[48] Catarina Mota. 2011. The Rise of Personal Fabrication. In *Proceedings of the 8th ACM Conference on Creativity and Cognition* (Atlanta, Georgia, USA) *(C&C '11)*. Association for Computing Machinery, New York, NY, USA, 279–288. https://doi.org/10.1145/2069618.2069665

[49] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy expectations and preferences in an IoT world. In *Thirteenth Symposium on Usable Privacy and Security*. 399–412.

[50] Sarah Prange, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. 2021. PriView – Exploring Visualisations Supporting 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. https://doi.org/10.1145/3313831.3376840

[51] Jun Rekimoto. 2002. SmartSkin: An Infrastructure for Freehand Manipulation on Interactive Surfaces. In *Proc. SIGCHI Conference on Human Factors in Computing Systems (CHI '02)*. ACM, 113–120.

[52] Martin Schrepp, Andreas Hinderks, and Jörg Thomaschewski. 2014. Applying the User Experience Questionnaire (UEQ) in Different Evaluation Scenarios. In *Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience (Lecture Notes in Computer Science, Vol. 8517)*, Aaron Marcus (Ed.). Springer International Publishing, Cham, USA, 383–392. https://doi.org/10.1007/978-3-319-07668-3_37

[53] William Seymour, Martin J. Kraemer, Reuben Binns, and Max Van Kleek. 2020. Informing the Design of Privacy-Empowering Tools for the Connected Home. 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, 1–14. https://doi.org/10.1145/3313831.3376264

[54] Joseph Shams, Nalin A. G. Arachchilage, and Jose M. Such. 2020. Vision: Why Johnny Can't Configure Smart Home? A Behavioural Framework for Smart Home Privacy Configuration. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. 184–189. https://doi.org/10.1109/EuroSPW51379.2020.00033

[55] Akash Deep Singh, Luis Garcia, Joseph Noor, and Mani Srivastava. 2021. I Always Feel Like Somebody's Sensing Me! A Framework to Detect, Identify, and Localize Clandestine Wireless Sensors. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 1829–1846. https://www.usenix.org/conference/usenixsecurity21/presentation/singh

[56] Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I. Hong. 2020. I'm All Eyes and Ears: Exploring Effective Locators for Privacy Awareness in IoT Scenarios. 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, 1–13. https://doi.org/10.1145/3313831.3376585

[57] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. 2019. I Don't Own the Data": End User Perceptions of Smart Home Device Data Practices and Risks. In *Proc. of the Fifteenth Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, USA, 16 pages.

[58] Christian Tiefenau, Maximilian Häring, Eva Gerlitz, and Emanuel von Zezschwitz. 2019. Making Privacy Graspable: Can we Nudge Users to use Privacy Enhancing Techniques? arXiv:1911.07701 [cs.HC] https://arxiv.org/abs/1911.07701

[59] Elise van den Hoven, Evelien van de Garde-Perik, Serge Offermans, Koen van Boerdonk, and Kars-Michiel H. Lenssen. 2013. Moving Tangible Interaction Systems to the Next Level. *Computer* 46, 8 (2013), 70–76. https://doi.org/10.1109/MC.2012.360

[60] Alexandra Voit, Sven Mayer, Valentin Schwind, and Niels Henze. 2019. *Online, VR, AR, Lab, and In-Situ: Comparison of Research Methods to Evaluate Smart Artifacts*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300737

[61] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300428

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

[63] Eric Zeng and Franziska Roesner. 2019. Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*. 159–176. https://www.usenix.org/system/files/sec19-zeng.pdf

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