# Exploring Users' Mental Models and Privacy Concerns During Interconnected Interactions

MAXIMILIANE WINDL, LMU Munich, Germany and Munich Center for Machine Learning (MCML), Germany
MAGDALENA SCHLEGEL, LMU Munich, Germany
SVEN MAYER, LMU Munich, Germany

Fig. 1. Images of the interconnected scenarios we used in our online survey generated with Midjourney. They show streaming a movie with a smartphone to a smart TV, streaming music with a smartphone to a smart speaker, navigating with a smartphone connected to the infotainment system, streaming a video call to a smart TV, controlling smart lights with a smartphone, and controlling a smart thermostat with a smartphone.

Users frequently use their smartphones in combination with other smart devices, for example, when streaming music to smart speakers or controlling smart appliances. During these interconnected interactions, user data gets handled and processed by several entities that employ different data protection practices or are subject to different regulations. Users need to understand these processes to inform themselves in the right places and make informed privacy decisions. We conducted an online survey ($N = 120$) to investigate whether users have accurate mental models about interconnected interactions. We found that users consider scenarios more privacy-concerning when multiple devices are involved. Yet, we also found that most users do not fully comprehend the privacy-relevant processes in interconnected interactions. Our results show that current privacy information methods are insufficient and that users must be better educated to make informed privacy decisions. Finally, we advocate for restricting data processing to the app layer and better encryption to reduce users' data protection responsibilities.

Authors' addresses: Maximiliane Windl, LMU Munich, Frauenlobstr. 7a, Munich, 80337, Germany and Munich Center for Machine Learning (MCML), Frauenlobstr. 7a, Munich, 80337, Germany, maximiliane.windl@ifi.lmu.de; Magdalena Schlegel, LMU Munich, Munich, 80337, Germany, m.schlegel@campus.lmu.de; Sven Mayer, LMU Munich, Munich, 80337, Germany, info@sven-mayer.com.


ACM 2573-0142/2024/9-ART259
https://doi.org/10.1145/3676504

CCS Concepts: • **Security and privacy → Human and societal aspects of security and privacy**; • **Human-centered computing → Human computer interaction (HCI)**.

Additional Key Words and Phrases: privacy, privacy risks, smart homes, interconnected interactions

**ACM Reference Format:**
Maximiliane Windl, Magdalena Schlegel, and Sven Mayer. 2024. Exploring Users' Mental Models and Privacy Concerns During Interconnected Interactions. *Proc. ACM Hum.-Comput. Interact.* 8, MHCI, Article 259 (September 2024), 23 pages. https://doi.org/10.1145/3676504

## 1 INTRODUCTION

An extensive body of prior research discusses privacy risks and user concerns regarding smartphones and smart home devices. Yet, all these works focus on singular concerns and solutions, which fails to portray the real world accurately. Nowadays, we rarely use these devices independently but rather use our smartphones to stream music to a smart speaker, control our smart homes, or connect our phones to navigate while driving. During all these interconnected interactions, user data gets handled, processed, and potentially stored by several entities that employ different data protection practices or are subject to different regulations. It is vital for users to understand the inner workings of these interconnected processes to be able to inform themselves and, ultimately, make informed decisions. Thus, we raise the question: How should a user, for example, remember to check the privacy regulations of the smart speaker app when, according to their mental model, only the smartphone app is handling their data?

While prior research recognized the privacy risks and concerns introduced by interconnected IoT devices through a technical lens, no research so far investigating the user perspective, i.e., if users have accurate mental and if they associate privacy concerns with interconnected interactions [10, 48, 69]. In contrast, research up to this rather focuses on user concerns for smart home devices and smartphones separately. In the context of smartphones, prior research, for example, found that users are especially concerned about financial and physical loss [25, 26], location tracking [35], and about certain data types, such as login credentials [13, 25, 26], text messages [26] and contact information [18]. However, in the context of smart home devices, users are most concerned about devices transmitting data without explicit consent [38], always-listening devices [39], and about demographics, communication, and activity data getting collected [6]. Moreover, also the proposed solutions for better privacy protection focus on the individual domains, such as notification and control mechanisms tailored specifically to smart home devices [61, 64] or smartphones [7, 62].

This paper takes the first step toward holistic data protection by investigating users' mental models of how today's systems share and process private information during interconnected interactions. This is important as we need to foster awareness when there is a mismatch with reality. To tackle this research goal, we conducted a large-scale online survey with 120 participants. We presented users with concrete interconnected scenarios created by experts and their single-device variants to compare the results and see if there is a difference in users' perception between single-device and interconnected scenarios. We first asked qualitative questions to gauge users' general comprehension level. We asked participants to explain which concrete privacy risks could occur in the described scenarios, which entities are involved, and how and where they believed these risks would occur. Participants later revisited the scenarios to rate their concerns regarding all involved entities. We also asked about their overall privacy concerns in both rounds to see if reflecting on the scenario and receiving more information affected their concerns.

We found that most participants struggled to understand the privacy-relevant process of interconnected scenarios, resulting in faulty mental models. Moreover, participants were more concerned about the interconnected variants of the scenarios overall than the single-device ones. This means

that even though most users fail to voice their concrete concerns and how they originate, they still feel more uneasy during interconnected interactions. Therefore, our work shows that most current privacy awareness methods are insufficient in informing users about privacy practices as they are mostly (1) static, (2) have to be actively retrieved, and (3) require users to be aware of all involved entities to be able to inform themselves. We conclude by advocating for restricting data processing to the app layer to lift some of the data protection responsibility from the users. With that, this paper takes the first important step toward holistic data protection by understanding the interconnected complexity of smart device interactions.

## 2 RELATED WORK

We first report prior work on privacy risks and concerns in the context of smartphones and smart home devices to motivate our research gap before summarizing work on privacy notices and control.

### 2.1 Privacy Risks and Concerns

In the context of bystanders, prior work found that even though people are concerned about both types of devices, i.e., smartphones and smart home devices, they assign greater risks to smart home devices and, thus, also express greater privacy concerns. Moreover, bystanders' privacy concerns increased with higher location intimacy and looser social relationships with the device owner [63]. Prior research also found a diverging danger perception regarding different sensor types [63]. While most users express clear concerns towards cameras and microphones [11, 50], they consider temperature or motion sensors less concerning [63]. Even more, some users express clear skepticism that these sensors cause any privacy issues at all [9, 14, 67]. Yet, while prior research argued that interconnected smart homes pose additional privacy risks and concerns to users [10, 48, 69], there is no prior work so far focusing on the user perspective.

*2.1.1 Smart Homes.* Smart devices pose various privacy threats, such as the possibility of revealing identities [51], tracking user behavior [3], or disclosing the number of people in a household, including their sleeping and eating patterns [49]. Moreover, video surveillance systems can be exploited by injecting forged video streams or revealing possibly sensitive video content [51, 54]. Besides most users' inability to name such concrete vulnerabilities [28, 42, 43], many still report a sense of unease or concrete privacy concerns when in their vicinity. For example, users fear that personal data might be revealed without consent [38] or that devices might always be listening and sharing this data with third parties [39]. Regarding concrete data types, users report being most concerned about demographics, communication, and activity data [6]. Yet, whether users perceive data as sensitive depends on the specific context and can, therefore, change over time [37].

*2.1.2 Smartphones.* Prior research showed that smartphones pose several privacy risks, many of which originate from the installed applications. This can be applications that leak sensitive data [20] or malware that actively collects data, such as messages or account data, from infected phones [68]. Yet, even when an application is not malicious per se, it can cause privacy risks. For example, when it acts as a confused deputy [12, 23], i.e., accidentally allowing malicious applications to access resources or by being bundled with malicious advertisement libraries [29, 59]. Moreover, several applications request more permissions than are actually required to fulfill their functionality, causing unnecessary privacy threats [21].

Consequently, many users express concerns about their privacy when dealing with smartphones. Such concerns include who can access their data [17, 18], whereby prior research disagrees on whether third- or second-party data sharing induces more user concerns [32, 60]. Yet, users frequently mention companies selling data as a major concern [1, 25, 32]. In regards to specific data

types, users are concerned about login credentials [25, 26, 57], text messages [26], contact information [18], and GPS [25, 26, 35]. Another smartphone-specific concern of people is physically losing a device, leading to others having access to their data [13].

*2.1.3 Summary.* Prior research extensively discussed privacy risks and concerns. Yet, most of these investigations focused on individual devices while overlooking that smartphones and smart devices are often combined. Hence, we need to investigate users' mental models and privacy concerns when faced with interconnected interactions.

### 2.2 Privacy Notice and Control

Besides ongoing criticism, privacy policies remain one of the primary sources for informing users about privacy practices. The most prominent points of criticism are their length [46] and abstract legal language [44, 56], making it hard for users to engage with them meaningfully. Hence, research also proposed several improvements, the most promising one being privacy labels that provide privacy information in a more condensed and digestible manner [33]. While originally designed for mobile applications, they have also been adapted for the IoT space [19]. Besides these approaches adopted for both platforms, research also envisioned domain-specific privacy notice and control mechanisms.

*2.2.1 Smart Homes.* Thakkar et al. [61] developed and compared four different privacy awareness mechanisms for smart home devices, including ambient smart lights, a smart speaker, and a privacy dashboard. They conclude that different visualizations have different advantages; thus, which is best depends on the context. While participants perceived the ambient light as rather discreet, the data dashboard enabled detailed insights. In the context of smart devices, recent research discussed tangible control mechanisms [2, 15, 47, 64]. They emphasize the high understandability of tangible mechanisms, which instill trust and are inclusive, especially for people with low technological understanding [2, 64]. Hence, many participants especially desire such tangible mechanisms in sensitive locations, such as bathrooms [11].

*2.2.2 Smartphones.* The most common smartphone privacy awareness and control mechanism is in-situ permission pop-ups. While early research on smartphone permissions found that many users paid little attention to permissions and did not understand them properly [22, 34], newer research shows that users are generally well-informed about their meaning [52]. Other research on smartphone-specific privacy notices and controls suggests privacy dashboards. Here, recent research showed that users like having privacy control options available, even though they tend not to use them [7]. Overall, research showed that smartphone privacy notices should be best displayed during app use and not already in the app store to increase recall rates [5].

*2.2.3 Summary.* The domain-specific, as well as the current primary means of privacy notice and control for smart home devices and smartphones, i.e., privacy policies and labels, are static or device-specific. Thus, as of now, users need to be aware of the entity responsible for protecting their data during every point of interaction to engage with the respective privacy information.

## 3 HYPOTHESES

Smartphones are increasingly being used in combination with other smart devices to fulfill a wide range of functionalities, such as music or movie streaming. Yet, research so far has only investigated users' mental models of single devices while disregarding the interconnected complexities. Hence, to provide meaningful notice and consent, as the first step, we need to understand users' mental models of interconnected scenarios. We approach this through the following five hypotheses:

**H1** Prior research showed that users are concerned about their privacy when interacting with smartphones [18, 25, 26] and smart home devices [6, 38, 39]. Yet, their concerns differ between the platforms. While users are, for example, concerned about physically losing their phones in the context of smartphones [13], they fear always listening devices in the context of smart homes [39]. Hence, we assume these concerns will be added when both types of devices are used together in a scenario. Consequently, we set our Hypothesis 1 **(H1): Users are more concerned about interconnected than single-device scenarios.**

**H2** We know that users already struggle to formalize the concrete threats and dangers when interacting with a single smartphone or smart device [28, 42, 43]. Hence, we assume that the increased complexity caused by data sharing and processing between multiple devices will lead to users' inability to understand the internal processes. Hence, we set our Hypothesis 2 **(H2): Users can not fully comprehend the interconnected scenarios.**

**H3** Prange et al. [53] showed that users' willingness to share their physiological data decreased over the course of the study after participants had reflected on multiple use cases and had learned what could be inferred from the data. Based on these results, we also assume that participants' privacy concerns will increase once they reflect on them in-depth and receive more information (i.e., learn about the involved entities). Thus, we set our Hypothesis 3 **(H3): Reflecting on the interconnected scenarios will increase users' privacy concerns.**

**H4** Prior research found that familiarity reduces privacy concerns. Apthorpe et al. [4], for example, showed that familiarity with a smart device reduces privacy concerns, and in a study by Windl and Mayer [63], participants mentioned not being concerned about smartphones anymore due to their great familiarity. Hence, we set our Hypothesis 4 **(H4): Familiarity with a scenario reduces privacy concerns.**

**H5** Literature showed that which entities have access to one's data greatly influences privacy concerns [17] and that who data is shared with can have the biggest impact on sharing decisions [18]. Hence, we hypothesize that even though users might be unsure which entity is responsible for protecting their data, they are concerned about all involved entities. Consequently, our Hypothesis 5 (**H5)** states: **In interconnected scenarios, users are concerned about all involved entities.**

## 4 SURVEY

We conducted an online survey with 120 participants to investigate our hypotheses. As we anticipated it would be hard for laypersons to grasp the concept of interconnected interactions, we first conducted expert interviews to create six concrete scenarios. We then used an iterative process to create the final survey. For that, we piloted the survey with colleagues, revised the questions based on their feedback, and then ensured the correct understanding by testing the survey with ten participants from Prolific.

### 4.1 Interconnected Scenario Creation

We conducted open interviews with eight HCI researchers (three female and five male) who were not involved in this paper to generate concrete interconnected scenarios for the survey. Three were postdocs and five PhD students (at least in their second year), and all worked in an HCI research department. Their ages ranged from 25 to 33 years ($M$ = 29, $SD$ = 2.92) and their affinity to technology (ATI) [24] was *M=4.8* (*SD=.6*). We interviewed HCI researchers as they are equally versed in technological and user understanding due to the interdisciplinary nature of HCI research. Moreover, interconnected interactions might be a novel concept to most people; thus, running Prolific studies, as done by prior work to gather scenarios (e.g., Windl et al. [65]), is unlikely to yield diverse and innovative scenarios. After introducing interconnected interactions briefly, we

asked the experts to envision at least two concrete scenarios they considered most common and relevant. We recorded and transcribed all interviews. Then, two researchers independently coded all statements, after which a third researcher joined to form groups of related codes using Affinity Diagramming [30].

Our analysis led to six scenario groups. Music Streaming (8) and Video Streaming (6), referring to streaming music, movies, or meetings from smartphones to smart speakers or smart TVs. Lights (5) and Thermostat (4), describing controlling lights or a thermostat with the smartphone, and Car (3), where experts discussed connecting the phone to the car's infotainment system for navigation and entertainment purposes. Moreover, experts discussed File Sharing (3) between devices, for example via Airdrop, and storing and accessing data and files in the Cloud (2). Yet, we did not include the Cloud and File Sharing scenarios in our final survey as both did not contain a smart device. Further, we did not include all scenarios that were only mentioned once. Such special scenarios were, for example, a smart toothbrush connected to the smartphone or a smartphone-controlled aquarium. The experts talked about streaming movies or meetings and video calls in the Video Streaming group. Here, the streamed data greatly differs in sensitivity. Hence, we hypothesized that users might perceive them very differently and decided to include two scenarios for this group, i.e., a scenario where users stream a video call to a smart TV and one where they stream a movie. Hence, in the end, we had six different interconnected Scenarios: *Audio*, *Video*, *Call*, *Light*, *Thermostat*, and *Navigation*.

We wanted to investigate how users perceive the interconnected scenarios compared to interacting with single devices (**H1, H2**), so we created variations of each interconnected scenario where only one device was present. For example, we created a variation for the music streaming scenario where the user plays the music directly on the smart speaker and one where the user plays it directly on their smartphone. This led to three variations for all scenarios except for the Lights and Thermostat scenarios; as those do not make sense without the smart device, they only have two variations. Please refer to Table 1 in the Appendix for all scenario descriptions we used in the survey. We further generated images of all scenarios using Midjourney to make it easier for participants to immerse themselves in the situations. See Figure 1 for the images we used for the interconnected versions of the scenarios and Figure 8 for all other images.

### 4.2 Survey Construction

We phrased each self-defined question as a statement to which the participants had to rate their agreement on a slider ranging from *strongly disagree* to *strongly agree* on a 100-point scale. We used a scale without ticks to prevent the responses from converging around the ticks, cf. [45]. Moreover, we used visual analog scales instead of Likert scales since they not only lead to more precise responses and, thus, a higher data quality [27], but they also collect continuous data, which allows for more statistical tests [58]. To further ensure the quality of the data, we saved a timestamp after each section and included an attention check item, asking to set a slider to the right or left.

Our final questionnaire had four main blocks: 1) demographic questions, 2) questions about the participants' privacy awareness and affinity for technology using the IUIPC questionnaire [41] and the ATI scale [24], 3) questions about participants' familiarity with and ownership of the devices and apps, and 4) the main part of the survey that consisted of two rounds. The full questionnaire containing the exact wording of the questions and statements can be found in the Appendix in Section A.2.

As described previously, we used a between-subject design, meaning every participant was confronted with one of the six interconnected scenarios and its single-device variations. This part of the survey had two rounds as we wanted to gauge participants' understanding of the privacy-relevant processes (**H2**) and their unbiased privacy concerns before and after receiving

more information about the interconnected processes (**H1**). So, in the first round, we first presented the scenario using the generated image and a text description and asked about the participant's familiarity and privacy concerns using the following two slider items: *I am very familiar with this scenario* (Q1) and *I am very concerned with this scenario from a privacy perspective* (Q2). Then, on the next page, we asked four free-text questions about the scenario. In detail, we asked *what* privacy risks participants believed to occur in the scenario (Q3), *where* (i.e., at which point of the scenario) (Q4), and *how* these risks occur (Q5), and finally, *who* they believed to be responsible for protecting their data (Q6). We randomized the order of the scenarios, i.e., whether participants first saw the interconnected scenario or a single-device variation, to prevent order effects.

In round two, participants revisited the interconnected variation of their scenario. Now, we asked participants again who they believed to be responsible for protecting their data, but this time, we used slider items and concretely asked about all involved entities, e.g., the smart device's or phone's operating system or the app provider. Next, we asked participants to rate their concerns about each entity handling their data. After answering all questions, we asked again how privacy-concerning they believed the scenario to be.

### 4.3 Participants

We recruited a total of 139 participants through Prolific. Our only inclusion criteria were that they were at least 18 years old and spoke English fluently. Yet, we had to exclude 19 participants for the following reasons (exclusion criteria): They gave answers that logically did not make sense (e.g., they stated to be extremely concerned about the scenario but stated in the free text question that there were no privacy risks) (7), they gave intentionally low effort responses (4), they had expired demographic data on Prolific (2), they consistently rated everything with 0 (2), they did not follow the instructions correctly (2), or they completed the survey three standard deviations faster than the average (1). Hence, our final sample consisted of 120 valid responses (20 per Scenario).

We had 62 females, 57 males, and one non-binary participant, whose ages ranged from 20 to 63 years ($M = 34.6$, $SD = 10.2$). We recruited participants from four continents (Europe, America, Asia, and Africa) to foster higher ecological validity. The top five countries of residence are Spain ($N = 19$), South Africa ($N = 14$), Poland ($N = 11$), Greece ($N = 9$), and Portugal ($N = 9$). All participants were full-time employed. Their mean technical affinity, as measured by the ATI scale [24], was 4.2 ($SD = 0.8$). We used the IUIPC questionnaire [41] to gauge the sample's privacy awareness on 7-point scales (higher scores = more concerns). Here, participants rated their *Awareness* with a mean of 6.2 ($SD = 0.9$), *Control* with 5.5 ($SD = 1.0$), and *Collection* with 5.5 ($SD = 1.2$). In line with the interpretation by Hoyle et al. [31], the scores suggest a notable level of privacy concerns across all three dimensions. We also asked about participants' familiarity with the smart devices and apps we inquired about in the survey (see Section A.2 $\mathbf{Q_F}3$). The sample had a mean familiarity of 80.3 with the *smart TV*, 56 with the *smart speaker*, 48.1 with the *smart lights*, 38.5 with the *car infotainment system*, and 26.6 with the *smart thermostat*. They reported a familiarity above 80 for all apps, except for the smart thermostat (26.9) and smart lights app (44.1). The participants took, on average, 16 minutes to complete the survey and were compensated with 1.72 £.

## 5 RESULTS

We analyzed our quantitative data using Python and R and used Thematic Analysis [8] for our qualitative data. For this, two researchers independently coded 20% of the participant statements, after which a third researcher joined to discuss the codes and form a joint code book. One researcher then coded the rest of the statements before the three researchers met again to form code groups and themes through multiple rounds of discussions. We performed sanity checks to ensure our

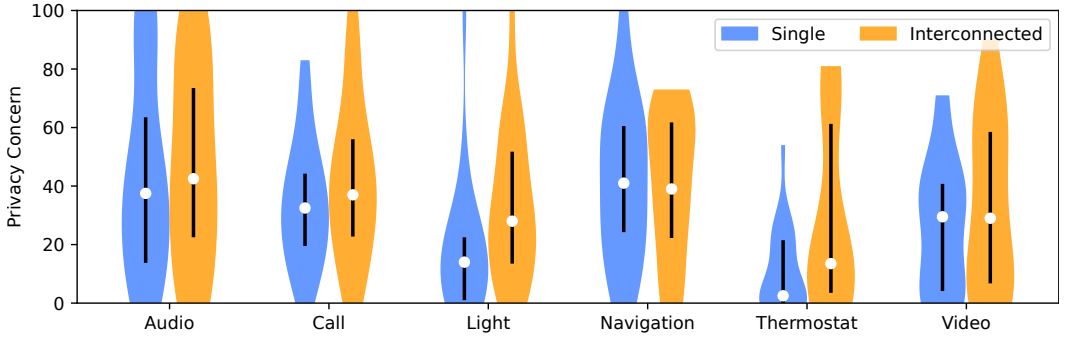



Fig. 2. The insights into the overall privacy concern per Interconnected scenario.

data quality through the exclusion criteria reported above. In the following, we describe the results of our five hypotheses.

### 5.1 H1: Overall Privacy Concern of Single vs. Interconnected Scenarios

First, we looked at the overall privacy concern (**Q2**) between the *Single* and the *Interconnected* scenarios, see Figure 2. A Shapiro-Wilk Normality Test showed that the *Privacy Concern* is not normally distributed ($W = 0.921$, $p < .001$). Thus, we used an ART ANOVA [66] that revealed a significant effect of Interaction and Scenario, ($F(1, 114) = 12.508$, $p < .001$, $\eta^2 = .099$; $F(5, 114) = 3.117$, $p < .011$, $\eta^2 = .12$; respectively); however, no interaction effect ($F(5, 114) = 1.013$, $p = .413$, $\eta^2 = .043$). This shows that participants perceived the interconnected scenarios as significantly more privacy-concerning than the single-device scenarios, which confirms our **H1**.

### 5.2 H2: Understanding of Interconnected Interactions

To investigate whether participants could fully comprehend the privacy-relevant processes within interconnected scenarios, three authors went through all qualitative responses for the interconnected scenarios and rated them on a scale from 1 to 5, whereby *1* meant that the participant either stated that they did not know the answer or put no effort into writing a feasible response, *2* that they tried to answer but the answer did not make sense or was very high-level, *3* that the person mentioned only one entity but described concrete and sensible privacy risks, *4* that the participant had a vague understanding that there was more than one entity involved, and *5* that the participant mentioned at least two involved entities and fully understood the concept and risks. We first coded 20% of the statements independently, after which we met to discuss and align our rating criteria. Then, we coded the rest of the statements and calculated the medians for each participant. Most (38.4%) participants received a rating of *3*, followed by *2* (27.8%), *4* (16.9%), *5* (12.12%), and finally *1* (4.7%). As we feared that this misunderstanding might have influenced the other questions, we performed a Kruskal-Wallis rank sum test, which showed no significant effect of the knowledge levels on the overall privacy concern (**Q2**), ($\chi^2(4) = 4.315$, $p > .365$, $\eta^2[H]$). This indicated that while participants might not understand where their subjective concern originates, their concern level is not significantly different from that of knowledgeable participants.

Next, we analyzed the qualitative responses to $Q3 - Q5$ to investigate this hypothesis further using the approach outlined in the introduction of this section. We calculated the number of unique codes per participant and aligned them with our rated levels of comprehension described in the previous paragraph. Hereby, we found a strong correlation using the Pearson coefficient between

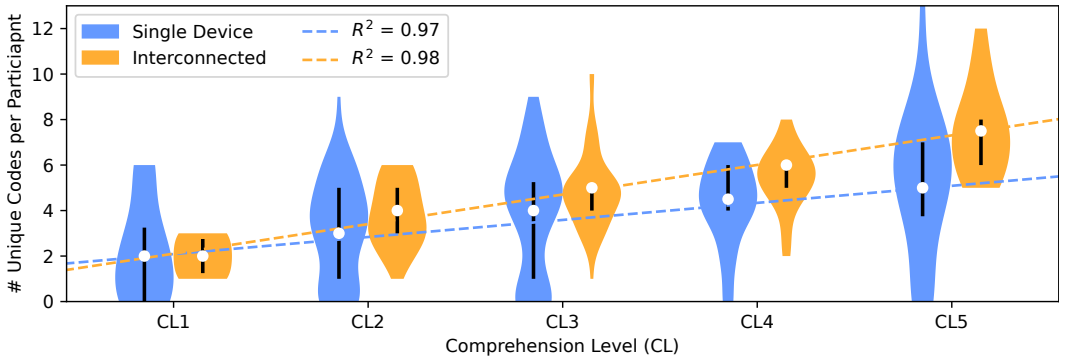



Fig. 3. The correlation of comprehension level and the number of unique codes.

the number of unique codes and the comprehension level, see Figure 3. This means that the more the participants understood the interconnected concept, the more details they gave when explaining the privacy threats. Our qualitative analysis led to the following five high-level themes: Who, How, Where, Data, and What, whereby each theme consists of multiple code groups, as illustrated in Figure 4. The numbers in each block indicate how often the code was mentioned in which category, whereby the first number stands for single-device and the second for the interconnected scenarios. While the figure shows that participants mentioned more concrete details in the single-device scenarios, this does not indicate that participants were more concerned in these scenarios. Rather, it shows that participants understood the single-device scenarios better and were, thus, able to come up with more concrete explanation. We use the same order (i.e., first single-device, second interconnected) when reporting the number of participants mentioning a specific aspect in the following. Moreover, we indicate our rated comprehension level (CL) in brackets after the participant number to contextualize the participant quotes.

***Who.*** describes which entities participants considered to be responsible for protecting their data. Most (S:88/I:65) participants believed that the *app provider* is responsible, as P5 (CL4) described in the interconnected scenario: *"The streaming app should limit the ability of the speaker to do anything other than play the music."* The second and third most frequently participants mentioned the *user* (S:61/I:41) and the *smart device company* (S:44/I:27). When describing that the *user* is responsible, participants most often wrote *"me"* or *"myself"* and P10 (CL2) simply stated: *"Stop talking private things while using [a] smartphone."* Interestingly, the *smartphone company* was mentioned way less frequently, with only 11 times for the single device and 16 times for the interconnected scenarios.

***How.*** illustrates what caused the privacy risk in the scenario. By far, most participants mentioned *audio recording* (S:44/I:22) as the cause of the privacy risk. P3 (CL2), for example, described the following in the single-device scenario: *"It not only records the command but other sounds or conversations as well."* As the second most frequent cause of privacy risks, participants mentioned *hacking* (S:30/I:18). *Inference*, and *signal intercept* were only mentioned in the interconnected scenarios. Here, P77 (CL4), for example, described the following scenario: *"Both devices can take notes and spy on you. Furthermore, they can communicate and even share data with each other, making the data pool even bigger."* In regards to *signal intercept*, P24 (CL3) feared that the *"video call data can be intercepted by a third party."*

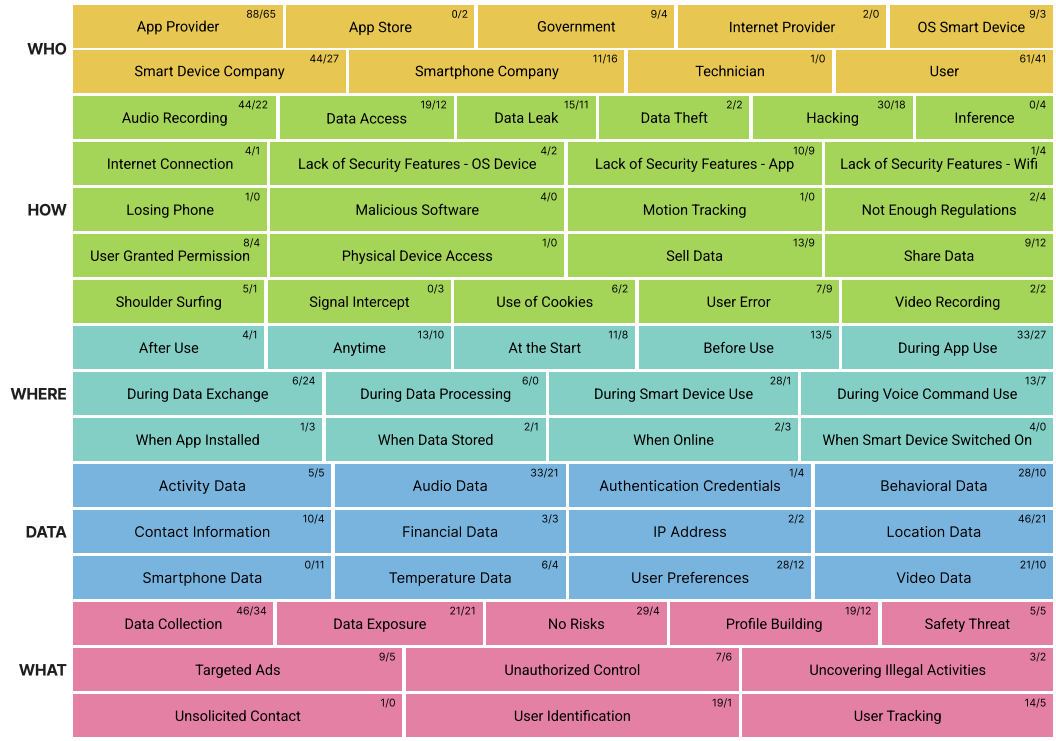



Fig. 4. The themes and code groups that resulted from our qualitative analysis. The numbers indicate how many times the code group was mentioned, whereas the first number represents the single device and the second the interconnected scenarios.

***Where.*** described at which point of the interaction participants believed the privacy risk to occur. Most (S:33/I:27) participants believed the privacy risk emerges *during app use*. For the single-device scenarios, participants mentioned *during smart device use* (S:28/I:1) second most frequently, and for the interconnected scenarios, participants mentioned *during data exchange* (S:6/I:24), as P109 (CL5) explains: *"the point would be when the mobile device sends the data to the TV."* In *at the start*, participants referred to the moment they opened the respective apps, and in *before use*, participants described moments, such as *"starting the car"* (P72, CL4) or *"after you agreed to their terms of service"* (P108, CL3).

***Data.*** encompasses all the different data types participants believed to get collected during the interaction. Most frequently, participants mentioned *location data* (S:46/I:21), *audio data* (S:33/I:21), *user preferences* (S:28/I:12), *behavioral data* (S:28/I:10), and *video data* (S:21/I:10). Regarding *behavioral data*, P88 (CL3), e.g., described: *"If someone could access that data, they could figure out when I'm home and when I'm not."* Interestingly, *smartphone data* was only mentioned in the interconnected scenarios (S:0/I:11). Here, participants feared that *"the car could access the data in my phone"* (P65, CL5), or generally that *"private data stored on the phone can be leaked to the app"* (P91, CL2).

***What.*** entails all the concrete privacy risks the participants mentioned. Here, most participants remained rather general and mentioned *data collection* (S:46/I:34), followed by *data exposure* (S:21/I:21), and *no risks* (S:29/I:4). In *safety threat*, participants feared that the data collected by the thermostat or smart lights might be abused to know when they are away to break into their

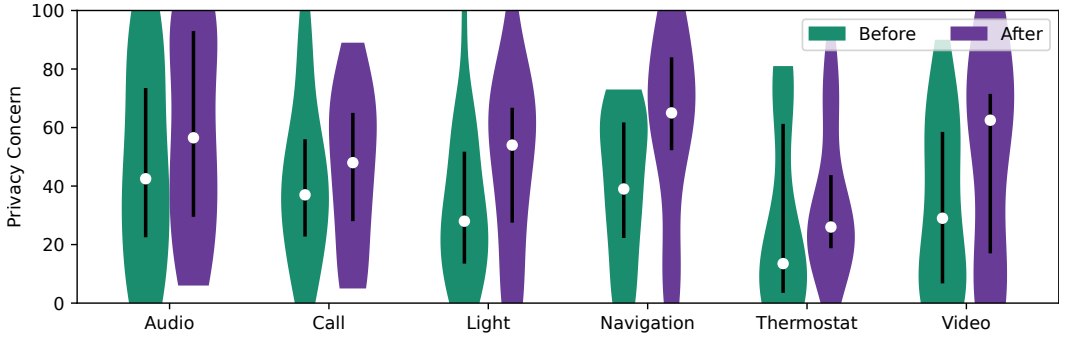



Fig. 5. Violin plots showing the change in participants' privacy concerns regarding interconnected interactions before and after they had received more information and reflected on the scenarios.

homes. In *uncovering illegal activities*, participants described scenarios such as that officials might uncover that they are *"watch[ing] illegal content"* (P117, CL4). In *unauthorized control*, participants feared that someone could hack their device and control it from afar, as P26 (CL3) describes: *"someone [can] obtain the control of the TV camera"* and in *unsolicited contact*, P37 (CL3), for example, feared to receive unwanted marketing calls.

We assigned most participants a comprehension level of *3*, and only 12.12% a rating of 5. This indicates that while most participants can grasp the privacy-relevant processes in single-device interactions, they mostly fail to understand interconnected scenarios fully. Moreover, we found that the higher the comprehension level, the more detail participants gave when describing risks, and that most concrete risks stemmed from a small but knowledgeable number of participants. Hence, we conclude that users can indeed not fully comprehend interconnected scenarios and accept **H2**.

### 5.3 H3: Influence of Reflection and Knowledge on Privacy Concerns

Next, we investigated whether more knowledge (**Q2** vs. **Q9**), i.e., after participants had reflected on the scenarios and received insights into the involved entities, leads to increased privacy concerns. As the data was not normally distributed ($W = 0.943$, $p < .001$), we conducted an ART ANOVA that showed that participants' privacy concerns were significantly higher ($F(1, 114) = 23.733$, $p < 001$, $\eta^2 = .173$) in the second round, see Figure 5. This observation is likely to be independent of the scenario, as the Scenario and the interaction effect are not statistically significant ($F(5, 144) = 1.477$, $p = 203$, $\eta^2 = .061$; $F(5, 114) = .880$, $p = .497$, $\eta^2 = .037$; respectively). Hence, we can confirm **H3**.

### 5.4 H4: Impact of Familiarity on Privacy Concern

We investigated this hypothesis from two perspectives, namely ownership ($\mathbf{Q_F1}$, $\mathbf{Q_F2}$) and familiarity ($\mathbf{Q_F3}$) with a technology and the scenario (**Q1**). While Figure 6a seems to indicate that owning the respective smart device leads to a slight decrease in privacy concerns, having the app installed seems to slightly increase the concerns (see Figure 6b). As the data was not normally distributed ($W = 0.906$, $p < .001$), we conducted two ART ANOVAs with Interaction as a random effect. Yet, they did not reveal significant differences between owning the smart device ($F(1, 118) = .389$, $p = .390$, $\eta^2 = .006$) and having the app installed or not ($F(1, 118) = 1.566$, $p = .213$, $\eta^2 = .013$).

To investigate whether familiarity with the individual devices and the apps significantly affected privacy concerns, we did correlation tests using the Pearson correlation. However, we did not find any correlations apart from a weak negative correlation between *smart tv* ($\rho = -0.23$, $p = 0.013$) and

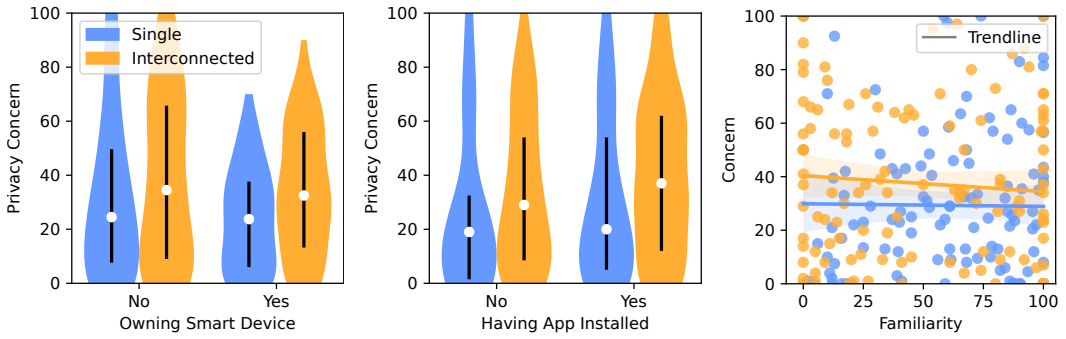
privacy concerns. Next, we looked at the familiarity between a scenario and privacy concerns; see Figure 6c. Yet, we did not find significant correlations. Altogether, we did not find strong evidence that familiarity reduces privacy concerns and, thus, reject our **H4**.

### 5.5 H5: Privacy Concerns Towards Different Entities

Lastly, we investigated about which involved entities participants were most concerned (**Q8**). Since the Shapiro-Wilk normality test showed that the data was not normally distributed ($W = 0.913$, $p < .001$), we conducted a Friedman test which revealed a significant difference between the five entities ($\chi^2(4) = 33.6, < .001, Kendall's\ W = .070$). We then used pairwise comparisons using the Wilcoxon signed rank test with Holm-Bonferroni corrections to find that participants were significantly more concerned about the app provider handling their data than all other entities (all $p < .01$). Moreover, participants were significantly more concerned about the OS of the smart device handling their data compared to the brand of the smartphone ($p < .01$), see Figure 7. All other comparisons were not statistically significant. Even though participants' concern levels were highest for the app provider and lowest for the smartphone brand, they were still high for all involved entities. Thus, we confirm **H5**.

## 6 DISCUSSION

Motivated by the fact that smartphones and smart devices are frequently used in combination, for example, to stream music or movies or control smart home devices, we conducted an online survey to find out if users have accurate mental models of the privacy-relevant processes in these interconnected interactions. While prior work recognized the privacy and security risks introduced by interconnected IoT devices, there is no research so far investigating user perception. Hence, to the best of our knowledge, this paper is the first to investigate users' mental models and privacy concerns in interconnected interactions. Our investigation found that apart from a small, knowledgeable group, most users have inaccurate mental models of the processes in interconnected interactions and struggle to understand how, where, and what privacy risks occur. Moreover, users express greater privacy concerns in the interconnected compared to single-device scenarios, and their concerns increased after reflecting on the scenario and receiving information about the involved entities. In the following, we discuss the impact of our results on future research and industry in light of our five hypotheses.




(a) Owning the smart device (b) App installed (c) Correlations

Fig. 6. a) The difference in privacy concerns when owning the smart device. b) The difference in privacy concerns was shown when the app was installed. c) Correlation between privacy concerns and familiarity.

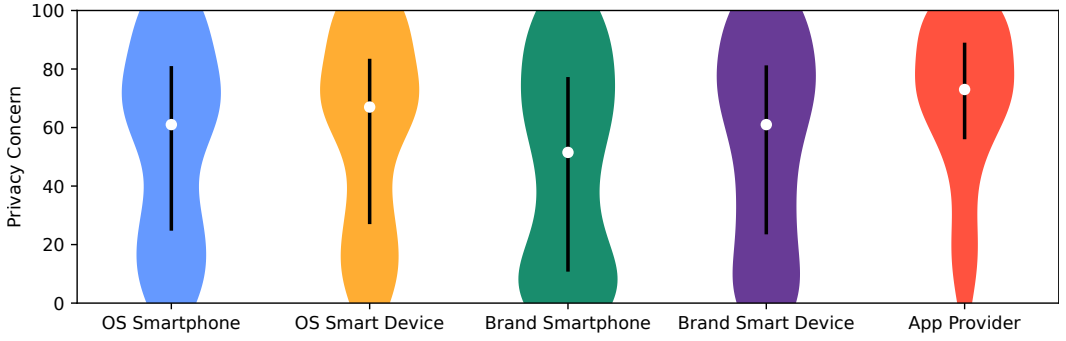



Fig. 7. Privacy concern towards different entities handling the data.

### 6.1 Users Have Facetted Privacy Concerns in Interconnected Scenarios

Our results confirm our hypothesis **H1** that participants express greater concerns in interconnected than in single-device scenarios. Moreover, users expressed the most concerns in the music streaming, video call, and navigation scenarios and fewer concerns in the smart thermostat and lights scenarios. This aligns with findings from prior work, where participants were most concerned about video and audio and least concerned about temperature and motion data [63]. Yet, the discrepancy in concerns regarding single and interconnected scenarios has multiple implications. On the one hand, this underlines that **it is important to give users options to inform themselves about privacy practices in interconnected scenarios to tackle these concerns and support them in making informed privacy decisions.** On the other hand, users being significantly more concerned in interconnected scenarios might not be justified. While more involved entities and sending data over networks might increase the risk of data mishandling or even data breaches, there are also significant privacy risks when only using smartphones. Researchers, for example, found that Xiamoi phones tracked user behavior and various device data and sent it to remote servers. Even though Xiamoi later denied the claims and released a software update, the researchers found that the data could easily be tracked back to individual users.[1] Such reports are concerning and underline the importance of educating users about the importance of installing software updates and being wary of what they agree to or which data they share to whom, independent of single-device and interconnected scenarios.

We could not confirm our **H4** that greater familiarity with a scenario reduces privacy concerns, as we found that both ownership and familiarity with a device had no significant influence on users' reported privacy concerns. Windl and Mayer [63] found that when users owned a device, their privacy concerns decreased, and in their qualitative findings, several participants mentioned not being concerned about smartphones due to their great familiarity. Yet, even though we found a slight trend that owning a device and being familiar with a scenario reduces concern, we did not find significant differences. We attribute this to the general greater complexity of the scenarios than what was described by Windl and Mayer [63].

Finally, we also confirmed our **H5** that users are concerned about all entities handling their private data, as all mean privacy concern scores were above 50. A promising approach to tackle these concerns would be to **restrict the data processing and handling to the app layer and to encrypt the traffic to other devices better to prevent attacks, such as deep package inspection. This would not only reduce the number of entities involved in data handling**

[1] https://www.forbes.com/sites/thomasbrewster/2020/04/30/exclusive-warning-over-chinese-mobile-giant-xiaomi-recording-millions-of-peoples-private-web-and-phone-use/

**and, with that, users' concerns but also lift the burden of taking care of data protection from the users.** Such efforts could be supported by government regulations that could advocate for stronger encryptions, similar to the telecommunication secret law in Germany. With that, concerns would be prevented before they arise. However, we must also consider the possible downsides of such stronger encryption, such as worse discoverability of new devices on device setup, which might lead to worse usability and result in poorer device adoption.

### 6.2 Users Have Inaccurate Mental Models of Interconnected Interactions

We could also confirm our hypothesis **H2** that users struggle to comprehend the interconnected scenarios fully, shown by the fact that most participants received a rating of 3 or 2 on their explanations, indicating that they have inaccurate mental models of the processes. This means that the current methods to inform users about privacy implications, i.e., privacy policies, are insufficient. While many providers worked on improving them by restructuring or enhancing them with visuals, privacy policies still require users to retrieve and engage with them actively. Yet, this becomes impossible if the user has an inaccurate mental model of what is happening, i.e., is unaware of all involved parties. Hence, **educating users about all involved entities and guiding them to find the relevant privacy information is essential. This will create a user base that conducts decisions that protect their data sovereignty.** One possible approach would be to visualize the data streams between the different devices to educate the users about the when and where of information transmission processes. For this, existing work on visualizations in smart homes can be leveraged, such as the work by Prange et al. [55], who used AR and VR to visualize the tracking space and sensor information of smart home devices. Similarly, **future research could use AR to visualize the data streams between smartphones and smart home devices.** With that, users could be educated about which entities handle their data at which points of the interaction. Besides visualizing the data streams with AR, leveraging smart home privacy dashboards suggested by Windl et al. [64] might be equally feasible. They placed dashboards in the entrance area of smart homes to visualize the location and sensors of smart devices. With this, bystanders can also inform themselves and take adequate measures if they feel concerned about their privacy. Such **smart home privacy dashboards could also be enhanced to show data streams between the devices and the different data actors.** This would bring the benefit of increasing the awareness of users and bystanders. Finally, the probably easiest-to-implement approach would be to do something similar to what is currently done with single sign-on or when users connect an account to another service on the web. The service would then ask if the user is sure to use this method as, for example, their email address, birthday, and user name are shared with the other entity. Leveraging a similar approach to this by **prompting users to agree to share certain kinds of information with other entities when they start an interconnected interaction might be a promising and comparably easy-to-implement approach.**

By comparing the users' reported privacy concerns between the first and second round, we further verified our **H3**, that users' concerns would increase once they reflected on the scenarios in-depth and received more information. This is promising as it suggests that users become more wary of privacy risks once they engage deeper with the topic, implying that our suggested education approach might indeed foster a more privacy-aware user base.

### 6.3 Limitations and Future Work

We used an online survey where we described scenarios using texts and generated images. With that, we hoped to make it easier for users to immerse themselves in the situations. While online surveys are an established method to gauge users' privacy concerns [40, 63], participants' responses might deviate from their real-world behavior [36]. In real life, privacy concerns are often not the

center of users' attention. Instead, users tend to weigh the increased convenience provided by the devices against potential privacy risks and will ultimately trade some of their privacy for an increased life quality [16]. Consequently, how participants perceive such real-life situations might differ and should be investigated in future research.

Our sample was relatively diverse as our participants stemmed from four different continents. With that, we hoped to achieve higher ecological validity of our results. However, we recruited our sample on Prolific, which, by nature, represents a specific subset of the population. Moreover, our findings might not hold true in the future. As people become more educated and familiar with devices, their mental models will likely evolve, which might also affect their concerns. Consequently, it will be interesting to repeat the survey in the future.

Moreover, we focused our investigation on a specific subset of potential scenarios that were generated by HCI researchers. While we hope to have covered various scenarios and devices, our selected scenarios were all about increasing comfort or providing entertainment. Yet, when smart devices are not used for increased comfort or entertainment but are essential to ensure the independence of, for example, elderly people, privacy concerns might be an even smaller concern for those affected. Hence, it would be interesting to investigate if our results hold, especially for different life contexts. In addition, we interviewed HCI researchers to create the scenarios as we assumed it would be hard for laypeople to grasp the concept of interconnected interactions and, thus, to create scenarios as innovative and diverse as the experts did. Yet, this also means that the scenarios might not be representative of those that laypersons or researchers with different expertise would have chosen.

Finally, our suggested approaches to educating users and helping them to find privacy information are not a silver bullet. Contrary, such approaches shift the burden of privacy protection to the user, which has recently been heavily criticized by privacy experts [65]. Instead, privacy experts suggested employing privacy by design approaches, which should prevent situations from violating users' privacy in the first place [65]. Yet, such disruptive changes require even more effort and especially incentives on the device and service provider side. Why should they implement such measures when users are currently willing to use the devices despite possible privacy violations? Here, we see it as the government's duty to issue appropriate regulations to enforce lasting change.

## 7 CONCLUSION

We conducted an online survey to investigate whether users have accurate mental models of the privacy processes in interconnected interactions, i.e., when smart devices and smartphones are not used alone but in combination with one another. We found that users consider scenarios more privacy-concerning when multiple data actors are involved. Yet, despite a small but knowledgeable user group, most fail to comprehend the privacy-relevant processes in interconnected interactions fully. Based on our results, we conclude that current privacy information methods are insufficient and that users have to be better educated to make informed privacy decisions. We further advocate for restricting data processing to the app layer and better encrypting device traffic to lift some of the data protection responsibility from the users.

## 8 OPEN SCIENCE

We encourage readers to reproduce and extend our results. Therefore, we made the data collected in our study and our analysis scripts available on the Open Science Framework https://osf.io/6dmgb/.

## REFERENCES

[1] Tanisha Afnan, Yixin Zou, Maryam Mustafa, Mustafa Naseem, and Florian Schaub. 2022. Aunties, Strangers, and the FBI: Online Privacy Concerns and Experiences of Muslim-American Women. In *Eighteenth Symposium on Usable*

*Privacy and Security (SOUPS 2022)*. USENIX Association, Berkeley, CA, USA, 387–406. https://www.usenix.org/system/files/soups2022-afnan.pdf

[2] 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

[3] Noah Apthorpe, Dillon Reisman, and Nick Feamster. 2017. A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic. In *Workshop on Data and Algorithmic Transparency*. arXiv, 6 pages. https://doi.org/10.48550/arXiv.1705.06805

[4] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 2, Article 59 (jul 2018), 23 pages. https://doi.org/10.1145/3214262

[5] Rebecca Balebako, Florian Schaub, Idris Adjerid, Alessandro Acquisti, and Lorrie Cranor. 2015. The Impact of Timing on the Salience of Smartphone App Privacy Notices. In *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices* (Denver, Colorado, USA) *(SPSM '15)*. Association for Computing Machinery, New York, NY, USA, 63–74. https://doi.org/10.1145/2808117.2808119

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

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

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

[9] 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, New York, NY, USA, 172–175. https://doi.org/10.1109/EISIC.2016.044

[10] Luigi Catuogno and Stefano Turchi. 2015. The Dark Side of the Interconnection: Security and Privacy in the Web of Things. In *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing* (Santa Catarina, Brazil). IEEE, New York, NY, USA, 205–212. https://doi.org/10.1109/IMIS.2015.86

[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. https://doi.org/10.1145/3411764.3445691

[12] Erika Chin, Adrienne Porter Felt, Kate Greenwood, and David Wagner. 2011. Analyzing inter-application communication in Android. In *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services* (Bethesda, Maryland, USA) *(MobiSys '11)*. Association for Computing Machinery, New York, NY, USA, 239–252. https://doi.org/10.1145/1999995.2000018

[13] Erika Chin, Adrienne Porter Felt, Vyas Sekar, and David Wagner. 2012. Measuring User Confidence in Smartphone Security and Privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C., USA) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 1, 16 pages. https://doi.org/10.1145/2335356.2335358

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

[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*. Gesellschaft für Informatik e.V., Bonn, Germany, 2 pages. https://doi.org/10.18420/muc2021-mci-ws09-393

[16] Tamara Dinev and Paul Hart. 2006. An extended privacy calculus model for e-commerce transactions. *Information systems research* 17, 1 (2006), 61–80. https://doi.org/10.1287/isre.1060.0080

[17] Aarthi Easwara Moorthy and Kim-Phuong L Vu. 2015. Privacy concerns for use of voice activated personal assistant in the public space. *International Journal of Human-Computer Interaction* 31, 4 (2015), 307–335. https://doi.org/10.1080/10447318.2014.986642

[18] Serge Egelman, Adrienne Porter Felt, and David Wagner. 2013. Choice architecture and smartphone privacy: There'sa price for that. *The economics of information security and privacy* (2013), 211–236. https://doi.org/10.1007/978-3-642-39498-0_10

[19] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the Experts: What Should Be on an IoT Privacy and Security Label?. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, New York, NY, USA, 447–464. https://doi.org/10.1109/SP40000.2020.00043

[20] William Enck, Damien Octeau, Patrick McDaniel, and Swarat Chaudhuri. 2011. A Study of Android Application Security. In *Proceedings of the 20th USENIX Conference on Security* (San Francisco, CA) *(SEC'11)*. USENIX Association, Berkeley, CA, USA, 21. https://www.usenix.org/legacy/event/sec11/tech/slides/enck.pdf

[21] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, and David Wagner. 2011. Android Permissions Demystified. In *Proceedings of the 18th ACM Conference on Computer and Communications Security* (Chicago, Illinois, USA) *(CCS '11)*. Association for Computing Machinery, New York, NY, USA, 627–638. https://doi.org/10.1145/2046707.2046779

[22] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android Permissions: User Attention, Comprehension, and Behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C., USA) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 3, 14 pages. https://doi.org/10.1145/2335356.2335360

[23] Adrienne Porter Felt, Helen J. Wang, Alexander Moshchuk, Steve Hanna, and Erika Chin. 2011. Permission Re-Delegation: Attacks and Defenses. In *20th USENIX Security Symposium* (San Francisco, CA) *(USENIX Security 11)*. USENIX Association, Berkeley, CA, USA, 16 pages. https://www.usenix.org/conference/usenixsecurity11/permission-re-delegation-attacks-and-defenses

[24] 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. https://doi.org/10.1080/10447318.2018.1456150

[25] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. 2022. Users' Expectations About and Use of Smartphone Privacy and Security Settings. 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 407, 24 pages. https://doi.org/10.1145/3491102.3517504

[26] Carol Fung, Vivian Motti, Katie Zhang, and Yanjun Qian. 2022. A Study of User Concerns about Smartphone Privacy. In *2022 6th Cyber Security in Networking Conference (CSNet)*. IEEE, New York, NY, USA, 1–8. https://doi.org/10.1109/CSNet56116.2022.9955623

[27] Frederik Funke and Ulf-Dietrich Reips. 2012. Why Semantic Differentials in Web-Based Research Should Be Made from Visual Analogue Scales and Not from 5-Point Scales. *Field Methods* 24, 3 (2012), 310–327. https://doi.org/10.1177/1525822X12444061

[28] 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, 5 pages. https://doi.org/10.5445/IR/1000083578

[29] Michael C. Grace, Wu Zhou, Xuxian Jiang, and Ahmad-Reza Sadeghi. 2012. Unsafe Exposure Analysis of Mobile In-App Advertisements. In *Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks* (Tucson, Arizona, USA) *(WISEC '12)*. Association for Computing Machinery, New York, NY, USA, 101–112. https://doi.org/10.1145/2185448.2185464

[30] Gunnar Harboe and Elaine M. Huang. 2015. Real-World Affinity Diagramming Practices: Bridging the Paper-Digital Gap. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 95–104. https://doi.org/10.1145/2702123.2702561

[31] Roberto Hoyle, Luke Stark, Qatrunnada Ismail, David Crandall, Apu Kapadia, and Denise Anthony. 2020. Privacy Norms and Preferences for Photos Posted Online. *ACM Trans. Comput.-Hum. Interact.* 27, 4, Article 30 (aug 2020), 27 pages. https://doi.org/10.1145/3380960

[32] Tun-Min Catherine Jai and Nancy J King. 2016. Privacy versus reward: Do loyalty programs increase consumers' willingness to share personal information with third-party advertisers and data brokers? *Journal of Retailing and Consumer Services* 28 (2016), 296–303. https://doi.org/10.1016/j.jretconser.2015.01.005

[33] 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

[34] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. 2012. A Conundrum of Permissions: Installing Applications on an Android Smartphone. In *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, Berlin, Heidelberg, 68–79. https://doi.org/10.1007/978-3-642-34638-5_6

[35] Predrag Klasnja, Sunny Consolvo, Tanzeem Choudhury, Richard Beckwith, and Jeffrey Hightower. 2009. Exploring privacy concerns about personal sensing. In *International Conference on Pervasive Computing*. Springer, Berlin, Germany, 176–183. https://doi.org/10.1007/978-3-642-01516-8_13

[36] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security* 64 (2017), 122–134. https://doi.org/10.1016/j.cose.2015.07.002

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

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

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

[40] Christoph Lutz and Aurelia Tamó-Larrieux. 2020. The robot privacy paradox: Understanding how privacy concerns shape intentions to use social robots. *Human-Machine Communication* 1 (2020), 87–111.

[41] 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. https://doi.org/10.1287/isre.1040.0032

[42] 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* (London, UK) *(EuroUSEC)*. Distributed System Security Symposium, Reston, VA, USA, 15 pages. https://doi.org/10.14722/eurousec.2018.23016

[43] 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), 22 pages. https://doi.org/10.2478/popets-2019-0068

[44] Elena Maris, Timothy Libert, and Jennifer R Henrichsen. 2020. Tracking sex: The implications of widespread sexual data leakage and tracking on porn websites. *New Media & Society* 22, 11 (2020), 2018–2038. https://doi.org/10.1177/1461444820924632

[45] Justin Matejka, Michael Glueck, Tovi Grossman, and George Fitzmaurice. 2016. The Effect of Visual Appearance on the Performance of Continuous Sliders and Visual Analogue Scales. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 5421–5432. https://doi.org/10.1145/2858036.2858063

[46] Aleecia M McDonald and Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* 4 (2008), 543–568. http://hdl.handle.net/1811/72839

[47] 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

[48] Sophia Moganedi and Jabu Mtsweni. 2017. Beyond the convenience of the internet of things: Security and privacy concerns. In *2017 IST-Africa Week Conference (IST-Africa)*. IEEE, New York, NY, USA, 1–10. https://doi.org/10.23919/ISTAFRICA.2017.8102372

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

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

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

[52] Anthony Peruma, Jeffrey Palmerino, and Daniel E. Krutz. 2018. Investigating User Perception and Comprehension of Android Permission Models. In *Proceedings of the 5th International Conference on Mobile Software Engineering and Systems* (Gothenburg, Sweden) *(MOBILESoft '18)*. Association for Computing Machinery, New York, NY, USA, 56–66. https://doi.org/10.1145/3197231.3197246

[53] Sarah Prange, Sven Mayer, Maria-Lena Bittl, Mariam Hassib, and Florian Alt. 2021. Investigating User Perceptions Towards Wearable Mobile Electromyography. In *Human-Computer Interaction – INTERACT 2021*. Springer International Publishing, Cham, 339–360. https://doi.org/10.1007/978-3-030-85610-6_20

[54] Sarah Prange, Sarah Delgado Rodriguez, Lukas Mecke, and Florian Alt. 2022. "I saw your partner naked": Exploring Privacy Challenges During Video-based Online Meetings. In *Proceedings of the 21st International Conference on Mobile*

*and Ubiquitous Multimedia* (Lisbon, Portugal) *(MUM '22)*. Association for Computing Machinery, New York, NY, USA, 71–82. https://doi.org/10.1145/3568444.3568468

[55] 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. https://doi.org/10.1145/3411764.3445067

[56] Robert W. Proctor, M. Athar Ali, and Kim-Phuong L. Vu. 2008. Examining Usability of Web Privacy Policies. *International Journal of Human-Computer Interaction* 24, 3 (2008), 307–328. https://doi.org/10.1080/10447310801937999

[57] Ismini Psychoula, Deepika Singh, Liming Chen, Feng Chen, Andreas Holzinger, and Huansheng Ning. 2018. Users' privacy concerns in IoT based applications. In *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*. IEEE, New York, NY, USA, 1887–1894. https://doi.org/10.1109/SmartWorld.2018.00317

[58] Ulf-Dietrich Reips and Frederik Funke. 2008. Interval-level measurement with visual analogue scales in Internet-based research: VAS Generator. *Behavior Research Methods* 40, 3 (01 Aug 2008), 699–704. https://doi.org/10.3758/BRM.40.3.699

[59] Bhaskar Pratim Sarma, Ninghui Li, Chris Gates, Rahul Potharaju, Cristina Nita-Rotaru, and Ian Molloy. 2012. Android Permissions: A Perspective Combining Risks and Benefits. In *Proceedings of the 17th ACM Symposium on Access Control Models and Technologies* (Newark, New Jersey, USA) *(SACMAT '12)*. Association for Computing Machinery, New York, NY, USA, 13–22. https://doi.org/10.1145/2295136.2295141

[60] Janice C Sipior, Burke T Ward, and Linda Volonino. 2014. Privacy concerns associated with smartphone use. *Journal of Internet Commerce* 13, 3-4 (2014), 177–193. https://doi.org/10.1080/15332861.2014.947902

[61] 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. https://doi.org/10.1145/3491102.3502137

[62] Priyanka Verma and Sameer Patil. 2021. Exploring Privacy Aspects of Smartphone Notifications. In *Proceedings of the 23rd International Conference on Mobile Human-Computer Interaction* (Toulouse & Virtual, France) *(MobileHCI '21)*. Association for Computing Machinery, New York, NY, USA, Article 48, 13 pages. https://doi.org/10.1145/3447526.3472065

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

[64] 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. https://doi.org/10.1145/3544548.3581167

[65] Maximiliane Windl, Verena Winterhalter, Albrecht Schmidt, and Sven Mayer. 2023. Understanding and Mitigating Technology-Facilitated Privacy Violations in the Physical World. 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 585, 16 pages. https://doi.org/10.1145/3544548.3580909

[66] Jacob O. Wobbrock, Leah Findlater, Darren Gergle, and James J. Higgins. 2011. The Aligned Rank Transform for Nonparametric Factorial Analyses Using Only Anova Procedures. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Vancouver, BC, Canada) *(CHI '11)*. Association for Computing Machinery, New York, NY, USA, 143–146. https://doi.org/10.1145/1978942.1978963

[67] 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

[68] Yajin Zhou and Xuxian Jiang. 2012. Dissecting Android Malware: Characterization and Evolution. In *2012 IEEE Symposium on Security and Privacy*. IEEE, New York, NY, USA, 95–109. https://doi.org/10.1109/SP.2012.16

[69] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle. 2014. Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks* 7, 12 (2014), 2728–2742. https://doi.org/10.1002/sec.795

# A APPENDIX

## A.1 Scenario Descriptions

Table 1. The scenario descriptions used in our online survey.

| Scenario | Condition | Description |
|---|---|---|
| Video | Only Smartphone | You want to watch an action movie, so you search for one in your preferred video streaming app on your smartphone. You find one and watch the movie on your smartphone. |
| | Only Smart Device | You want to watch an action movie, so you search for one in your preferred video streaming app on your smart TV. You find one and watch the movie on your smart TV. |
| | Interconnected | You want to watch an action movie, so you search for one in your preferred video streaming app on your smartphone. You find one and stream the movie to your smart TV to watch it on a bigger screen. |
| Audio | Only Smartphone | You are having a cozy day at home and want to listen to relaxing music. Thus, you tell your smartphone via voice command to play a fitting playlist using your favorite music streaming app. |
| | Only Smart Device | You are having a cozy day at home and want to listen to relaxing music. Thus, you tell your smart speaker via voice command to play a fitting playlist using your favorite music streaming app. |
| | Interconnected | You are having a cozy day at home and want to listen to relaxing music. Thus, you tell your smartphone via voice command to play a fitting playlist using your preferred music streaming app. As you want better sound quality, you decide to stream the music to your smart speaker. |
| Call | Only Smartphone | You are at home and notice that it is your friend's birthday, so you take your smartphone and call that friend via video call using your preferred video call app. |
| | Only Smart Device | You are at home and notice that it is your friend's birthday, so you turn on your smart TV that has an inbuilt camera and call that friend via video call using your preferred video call app. |
| | Interconnected | You are at home and notice that it is your friend's birthday, so you take your smartphone and call that friend via video call using your preferred video call app. Unfortunately, your smartphone battery is about to run out, so you continue the video call on your smart TV that has an inbuilt camera. |
| Thermostat | Only Smart Device | You are a little cold while working from your home. You go to your smart thermostat and set it three degrees warmer. |
| | Interconnected | You are a bit cold while working from your home. You use your smartphone to set the smart thermostat three degrees warmer in your preferred smart thermostat control app. |
| Navigation | Only Smartphone | You want to drive to a friend in your car, so you use your smartphone to enter the address into a navigation app. As soon as the phone is safely stored in the phone holder, you start the navigation, which guides you to your friend's house on the fastest route. |
| | Only Smart Device | You want to drive to a friend in your car, so you use your car infotainment system to enter the address into a navigation app. It then guides you to your friend's house on the fastest route. |
| | Interconnected | You want to drive to a friend in your car, so you use your smartphone to enter the address into a navigation app. You connect your smartphone to the car infotainment system, which then guides you to your friend's house on the fastest route. |
| Lights | Only Smart Device | You want to go to bed and turn off the smart lights. Therefore, you click on the wireless controller, which is from the same company as your smart lights, to turn them off. |
| | Interconnected | You want to go to bed and turn off the smart lights. You use your smartphone to remotely turn off the smart lights using your preferred smart lights control app. |

## A.2 Questionnaire

### *A.2.1 Demographics.*

**$Q_G$1** In which country do you currently live? [drop-down list]
**$Q_G$2** In which country were you born? [drop-down list]
**$Q_G$3** Which gender do you most identify with? [single choice]
- Male
- Female
- Non-binary
- Self-described

**$Q_G$4** How old are you? [number field]
**$Q_G$5** What is the highest degree you have received? [single choice]
- Less than high school degree

- High school graduate
- Some college but no degree
- Bachelor's degree
- Master's degree
- Doctoral degree
- Vocational education

**$Q_G$6** What is your current primary occupation? [free text]

### *A.2.2 Privacy Perception & Affinity For Technology.*

*IUIPC.* Many people spend a lot of time online, for example, on their smartphones, tablets, or computers. During this time online, people also share data, for example, when signing up for online shopping, posting on social media, or using GPS in navigation apps. In the following questions, we are interested in your personal experience and perception when sharing your personal information online. Please indicate the degree to which you agree/disagree with the following statements. [7-point Likert scales from strongly disagree to strongly agree].

**$Q_G$7** I have been the victim of what I felt was an improper invasion of privacy.
**$Q_G$8** I am very concerned about the privacy of my data.
**$Q_G$9** I always falsify personal information needed to register with some websites.
**$Q_G$10** It usually bothers me when online companies ask me for personal information.
**$Q_G$11** When online companies ask me for personal information, I sometimes think twice before providing it.
**$Q_G$12** It bothers me to give personal information to so many online companies.
**$Q_G$13** I'm concerned that online companies collect too much personal information.
**$Q_G$14** Your online privacy is really a matter of your right to exercise control and autonomy over decisions about how your information is collected, used, and shared.
**$Q_G$15** Your control of your personal information lies at the heart of your privacy.
**$Q_G$16** I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.
**$Q_G$17** Companies seeking information online should disclose the way the data are collected, processed, and used.
**$Q_G$18** A good consumer online privacy policy should have a clear and conspicuous disclosure.
**$Q_G$19** It is very important to me that I am aware and knowledgeable about how my personal information will be used.

*ATI.* On this page, we are interested in how you deal with technology. Please indicate the degree to which you agree/disagree with the following statements. [6-point Likert scales from completely disagree to completely agree]

**$Q_G$20** I like to occupy myself in greater detail with technical systems.
**$Q_G$21** I like testing the functions of new technical systems.
**$Q_G$22** I predominantly deal with technical systems because I have to.
**$Q_G$23** When I have a new technical system in front of me, I try it out intensively.
**$Q_G$24** I enjoy spending time becoming acquainted with a new technical system.
**$Q_G$25** It is enough for me that a technical system works; I don't care how or why.
**$Q_G$26** I try to understand how a technical system exactly works.
**$Q_G$27** It is enough for me to know the basic functions of a technical system.
**$Q_G$28** I try to make full use of the capabilities of a technical system.

### *A.2.3 Ownership & Familiarity with Devices and Apps.*

**$Q_F$1** Which of the following devices do you own? [multiple choice]
- (a) Smartphone
- (b) Smart TV
- (c) Smart Speaker
- (d) Car Infotainment System
- (e) Smart Thermostat
- (f) Smart Lights

**$Q_F$2** Which of the following apps do you have installed? [multiple choice]
- (a) Music streaming app
- (b) Video streaming app
- (c) Video call app
- (d) Navigation app
- (e) Smart thermostat control app
- (f) Smart lights control app

**$Q_F$3** I am very familiar with the following technology. [slider]
- (a) Smartphone
- (b) Smart TV
- (c) Smart Speaker
- (d) Car Infotainment System
- (e) Smart Thermostat
- (f) Smart Lights
- (g) Music streaming app
- (h) Video streaming app
- (i) Video call app
- (j) Navigation app
- (k) Smart thermostat control app
- (l) Smart lights control app

*A.2.4 Main Part of Survey.* In the following, we will confront you with some scenarios. Please immerse yourself in the situation and answer the questions accordingly. [Following block repeated for all scenario variations].

*Round 1.* Immerse yourself in the following situation: [scenario image] [scenario text description].

**Q1** I am very **familiar** with this scenario. [slider]
**Q2** I am very **concerned** with this scenario from a privacy perspective. [slider] [page break]
**Q3** **What privacy risks** can occur in this scenario? Please describe in at least one sentence. [free text]
**Q4** **Where** do you think **privacy risks** can occur in this scenario (i.e., at which point of the interaction)? Please describe in at least one sentence. [free text]
**Q5** **How** do you think **privacy risks** can occur in this scenario (i.e., what causes these risks)? Please describe in at least one sentence. [free text]
**Q6** **Who** do you think is **responsible** for **protecting your private data** in this scenario? [free text]

Thank you very much for providing your feedback for the first phase of the survey. Now, you will revisit one of the scenarios again. [Following block is only shown for the interconnected scenario variation]

*Round 2.* Immerse yourself in the following situation: [scenario image] [scenario text description]

**Q7** I strongly believe the following entity is **responsible** for **protecting my private data** in this scenario. [slider]
- Operating system of [smart device]
- Operating system of smartphone
- Provider of [app]
- Brand of [smart device]
- Brand of smartphone

**Q8** I am very **concerned** about the following entities **handling my data**. [slider]
- Operating system of [smart device]
- Operating system of smartphone
- Provider of [app]
- Brand of [smart device]
- Brand of smartphone

**Q9** I am very **concerned** with this scenario from a privacy perspective. [slider]

Fig. 8. Images of the single device variants of the example scenarios we used in our online survey generated with Midjourney. From left to right, top to bottom, they show watching a movie on a smart TV, watching a movie on a smartphone, listening to music with a smart speaker, listening to music with a smartphone, controlling smart lights, having a video call on a smart TV, having a video call on a smartphone, navigating with the car's infotainment system, navigating with a smartphone, controlling a smart thermostat.

Received February 2024; revised May 2024; accepted June 2024