Karola Marky*, Nina Gerber, Michelle Gabriela Pelzer, Mohamed Khamis, and Max Mühlhäuser

"You offer privacy like you offer tea": Investigating Mechanisms for Improving Guest Privacy in IoT-Equipped Households

Abstract: IoT devices are becoming more common and prevalent in private households. Since guests can be present in IoT-equipped households, IoT devices can pose considerable privacy risks to them. In this paper, we present an in-depth evaluation of privacy protection for guests considering the perspectives of hosts and guests. First, we interviewed 21 IoT device owners about four classes of mechanisms obtained from the literature and social aspects. Second, we conducted an online survey (N=264) that investigates the perspective of guests in IoT-equipped households. From our results, we learn that protection mechanisms should not introduce privacy threats and require low resources. Further, hosts should keep control over their devices and the aesthetics of their living spaces. Guests, however, value feedback about the status of privacy protection which can interfere with aesthetics. Privacy protection should rather foster collaboration and not impact the visit of the guest too severely. We use our results to identify a design space for guest privacy protection in IoT-equipped households.

Keywords: IoT Privacy, Bystander Privacy, Privacy Protection Mechanisms

DOI 10.56553/popets-2022-0115
Received 2022-02-28; revised 2022-06-15; accepted 2022-06-16.

***Corresponding Author: Karola Marky:** Leibniz University Hannover and University of Glasgow, E-mail: karola.marky@itsec.uni-hannover.de
Nina Gerber: Technical University of Darmstadt, E-mail: nina.gerber@tu-darmstadt.de
Michelle Gabriela Pelzer: Technical University of Darmstadt, E-mail: michelle_gabriela.pelzer@stud.tu-darmstadt.de
Mohamed Khamis: University of Glasgow, E-mail: mohamed.khamis@glasgow.ac.uk
Max Mühlhäuser: Technical University of Darmstadt, E-mail: max@informatik.tu-darmstadt.de

1 Introduction

Internet of Things (IoT) devices in private households are getting more popular and versatile based on the benefits offered by their sensing capabilities. However, privacy concerns based on the sensing capabilities have repeatedly been demonstrated [2, 6, 11, 21, 47, 50] creating a need for privacy protection mechanisms [51, 52]. In this paper, we investigate privacy protection for *guests* in IoT-equipped households.

Implementing privacy protection for guests constitutes a particular challenge for two main reasons: First, guests might not be aware of IoT devices and their data collection capabilities [26, 33, 41, 49]. Second, privacy protection for guests requires cooperation of *hosts* – the owners of the IoT devices – since they mostly install and configure the protection mechanisms. This aspect results in a power imbalance [26, 50] since hosts are not always willing to disclose IoT devices or change their settings to accommodate guests [12]. Because of that, we investigate the perspectives of *hosts* and *guests* focusing on the following research questions:

RQ1: What are essential requirements for guest privacy protection mechanisms? We want to understand how privacy protection mechanisms for guests should be designed for wide adoption by hosts and guests.

RQ2: Which factors impact the intent of using privacy protection mechanisms for guests? We want to understand why hosts and guests would (not) use mechanisms and which factors impact their decision.

RQ3: Who is perceived to be responsible for guest privacy protection in IoT-equipped household? We investigate expectations and perceptions from the social level on who is responsible for offering privacy protection for guests.

RQ4: How and why do or should hosts disclose their IoT devices to guests? Here, we investigate aspects of device disclosure including the reactions of guests.

Based on a literature search on existing guest privacy mechanisms, we designed two consecutive user studies – one considering the host perspective and one considering the guest perspective. In the first study,

we interviewed 21 owners of IoT devices about their past experiences with accommodating close friends and captured their perceptions of privacy protection mechanisms that support guest privacy. We used the results from the first study to inform an online survey (N=264) that investigated the guest perspective.

Overall, we learned that the perspectives of hosts and guests demonstrate several differences that might conflict with each other. For instance, guests prefer salient mechanisms that support their awareness while hosts consider aesthetic aspects of their living space, which might interfere with salience.

We use the results of our investigation and related work to identify a design space for guest privacy protection in IoT-equipped household. Our design space considers data required for the privacy mechanism to run, the scope of privacy protection, the effect on IoT devices, user involvement, financial burden, burden on social aspects, the composition of privacy protection, control of mechanisms, and feedback.

Research Contribution

1. An in-depth investigation of guest privacy mechanisms for IoT-equipped household considering the perspectives of hosts and guests.
2. Detailed results from both perspectives, including user expectations, requirements, impact factors, reasons for (not) using privacy protections for guests, as well as responsibility considerations.
3. A design space for guest privacy protection mechanisms that accommodate user expectations, privacy preferences, and considers the social level.

2 Background and Related Work

To set the scene for our work, we report research on bystander privacy since guests form a subgroup of bystanders [33, 49] and guest privacy mechanisms.

2.1 Investigations of Bystander Privacy

Guests are individuals that are temporarily staying in the home of another individual. Guests can be considered a special case of bystanders. *Bystanders* are any third party that could be affected by a technology [41].

Occupants of IoT-Equipped Households. *Occupants* living in the same household, such as partners, form one group of bystanders. Study participants stated conflicts might arise due to different privacy attitudes of hosts and other occupants [10]. However, privacy aspects can be negotiated over time [19], but social relations make this difficult [48]. In the worst case, information from IoT devices might be used to harm individuals, e.g., by accessing recorded information to impersonate them [18]. Children form a special group of occupants. IoT devices might result in tension between parents and children because parents might use information from IoT devices to fulfill their responsibilities which might feel like surveillance for children [10, 35, 36, 46].

Household Aids in IoT-Equipped Households. The second group of bystanders is given by people who work in foreign households, such as repair or household assistance. An investigation of privacy perceptions of nannies showed that they differentiated between private actions which should not be monitored and professional activities which could be allowed for monitoring [4].

Guests in IoT-Equipped Households. *Guests*, such as friends or relatives, are the last group of bystanders. It has been shown that guests wish to be aware of the data collection to give their consent [1, 32, 33, 49]. When making privacy decisions, guests consider familiarity with the household and their relation to the host [32]. This was also shown for the perspective of hosts. The relation to the guests can impact the host's decision to disclose IoT devices [10]. Guests further consider the purpose of IoT devices, e.g., surveillance cameras can be acceptable depending on their location [42]. Considering overall usage of IoT devices, guests tend to trust hosts regarding device installation and management [25].

The presence of guests can also impact host privacy since guests could observe notification output. Hence, hosts wish to tailor device configuration to the presence of guests [33, 51]. Furthermore, users of smart speakers might listen to audio recordings of other occupants, children, or guests, posing a privacy risk for them [26]. Cobb et al. investigated incidental users – including guests and occupants – in terms of potential privacy implications, reactions, and solutions for privacy risks and the host's willingness to accommodate needs of incidental users [12]. Overall, they found that incidental users wish to be informed about device presence, devices should include mechanisms that motivate a conversation between hosts and incidental users. Finally, devices should offer a mode that offers the comfort given by the device without violating privacy.

Guests in IoT-Equipped Rental Homes. Another stream of research specifically considered guests in private households that are rented, e.g., AirBnBs [31, 44]. Here, specific mechanisms to support the guests were proposed. This paper extends this existing body of work by specifically investigating privacy protection mechanisms for guests from two distinct perspectives.

2.2 Guest Privacy Mechanisms

Several measures for supporting guest privacy are available in the literature. We clustered the mechanisms from the literature into the following four categories:

1) Visibility and Transparency: The first category consists of measures that aim to increase visibility and transparency of IoT devices. *Device disclosure* forms the first measure in this category. It can be realized by *verbal information* from the host [31, 50], or by *notifications* that guests receive on personal devices [13, 51]. Another measure is given by *status or location indicators* [1, 32, 44, 45, 50, 51]. Yao *et al.* suggest *labeling* IoT devices with QR-codes that link to privacy information [49]. Besides measures that affect individual devices, a *dashboard* that visualizes all devices in a specific way can give an overview [31].

2) Privacy Settings: The second category is given by letting guests access and change privacy settings. This can be realized through a *guest mode* that lets bystanders interact with the device [16, 19, 23, 26, 33, 51]. Using this mode, the guests can adjust privacy settings. Further, no data of guests is stored when using a device in guest mode [26]. The *access to privacy settings* could also be given without a specific guest mode or in *cooperation* with the owner [49, 51].

3) Data Filtering and Deletion: Our third category is related to *filtering* or *deleting* data. Devices could be designed to recognize guests and do not save their data [10, 26] or send a noise that masks conversations with guests [28]. Filtering can also be realized by manipulating the stored data, such as blurring faces of guests [22]. Another option that allows for interaction with the device without reduction of functionality is deleting data after the visit [33].

4) Personal Privacy Assistance: The final category is given by *personal privacy assistance* meaning that guests use supportive software on a personal device [13–15]. The software can be tailored specifically to the guest's preferences.

3 Study I: Host Perspective

Our first study investigates how hosts evaluate privacy protection for their guests. For this, we provided the participants with the mechanisms presented in Sect. 2.2 to capture their perspectives on them. We aimed to use the participants' perceptions on why (not) using a presented mechanism to gather host expectations. For this, we conducted semi-structured interviews with 21 IoT device owners with an average duration of 45 minutes (min=25, max=82). All participants took part voluntarily and were not compensated. Due to COVID-19, the interviews were held via the open-source video-calling software "BigBlueButton" [5]. Video calls are considered an appropriate instrument for collecting qualitative interview data during the pandemic [29]. The interviews were audio-recorded and transcribed for analysis. The methodology conforms to all requirements of our institution's ethics commission.

Procedure. The interviews consisted of five main parts. For the interview questions, we refer the reader to Appendix A. First, participants were welcomed and thanked for participation. They received a PDF consent form and were asked to read and sign it digitally or printed and scanned. They were then introduced to the study scenario. We provided a short definition of IoT devices [3] and asked participants to imagine a situation where a good friend visited them at home specifically instructing participants to consider the time before the COVID19 lockdown. Next, we made sure that the participants understood the IoT definition, the scenario and that they should consider their own point of view. Second, we asked participants about their IoT devices, including use cases, past usage, and plans to purchase other devices. Third, we focused on participants' experiences with guests in their IoT-equipped households, such as reactions from guests and whether they had drawn their guests' attention towards the IoT devices.

Fourth, we used presentation slides as a standardized way to introduce privacy protection mechanisms for guests considering the four different categories outlined in Sect. 2.2: (1) mechanisms for visibility and transparency, (2) mechanisms that offer privacy settings or a guest mode, (3) mechanisms for filtering or deleting collected data, and (4) the concrete implementation of in the form of personal privacy assistance. The presentation slides were chosen to help participants comprehend the mechanisms. They could read the information at their own pace. We asked our participants to evaluate

ID	age	gender	occupation	IoT Devices
P1	32	m	PhD student	vacuum robot, TV
P2	30	f	administrative staff	Alexa, speakers, lights
P3	35	f	scrum master	Alexa, smart speaker, surveillance cameras, Router
P4	42	m	clerk	TV, gaming console (with camera and microphone)
P5	34	m	strategic energy planer	Sonos, Philips Hue, voice controller, Alexa
P6	25	m	student	Musikbox, Fire-Stick with voice control
P7	30	m	data scientist	Alexa, Chromecast
P8	35	f	student	vacuum robot, heating system, door camera
P9	29	m	software developer	Alexa
P10	32	m	student	Alexa, surveillance camera, lights, Siri
P11	34	m	business analyst	Google Home
P12	33	m	project coordinator	Alexa
P13	31	m	computer scientist	vacuum robot, 3 Alexa devices, 2 Echo 8 devices, power plugs
P14	26	m	PhD student	Alexa, Philipps Hue with hub, doorlock, Intercom, power plug
P15	30	f	art director	Google Home*
P16	25	m	developer	lights, window blinds, vacuum robot, Alexa
P17	24	m	none	TV with microphone
P18	23	m	student	Google Home Mini, Alexa*
P19	23	other	student	Chromecast, Echo Dot*
P20	31	f	3D artist	Alexa, vacuum robot
P21	26	m	student	lights, vacuum robot, Homepod

Table 1. Demographics of the interview sample. IoT marked with a * were owned in the past.

each privacy protection mechanism. The mechanisms were introduced in randomized order given by a Latin square to avoid sequence effects, except for the privacy assistant, which differs from the other concepts in that it describes a concrete implementation. Based on trial interviews, we found that the participants would have the best chance to understand the concept if it is introduced this way. Finally, we asked about the effects of the privacy protection mechanisms discussed in terms of social interaction with guests and collected demographics. We then thanked the participants and gave them the opportunity to ask questions or make comments.

Participants. We recruited 21 participants from country blended for anonymity by mailing lists, social networks, and word-of-mouth. All participants were required to either currently own an IoT device that can capture audio or visual data of guests since those are perceived as most privacy-invasive [8, 27, 38] or to have owned it until recently. Twenty participants currently owned such a device, and one owned it in the past. The participants were on average 30 years old (min=23, max=42, SD=4.81, Md=30). Five participants identified as female, one as other, and the remainder as male. For detailed demographics, including the IoT devices, the reader is referred to Table 1.

Data Analysis. We analyzed the data using the thematic analysis methodology [7]. Two researchers independently familiarized themselves with the data by reading the transcripts repeatedly. Then, the two researchers independently conducted open coding to identify relevant themes and codes, one researcher on all and the other researcher on half of the transcripts. Afterward, the two researchers met to discuss, group, and structure the codes. They agreed on a shared codebook, which was used for the final round of coding. If questions arose or new codes came up during the coding process, the researchers met again to discuss any ambiguities. Saturation was reached after 15 participants. Due to the qualitative and exploratory orientation of our study, we deliberately refrain from reporting measures of inter-rater agreement [34]. Instead, we solved differences in the coding through discussion. This allowed us to iteratively refine the codebook as disagreements in the codings usually indicated fuzzy codes. The final codebook is provided in Table 4 in Appendix C.

Limitations. Like most qualitative and exploratory work, our interview study holds several limitations. First, as interviews rely on self-reported data, they may be subject to social desirability, availability bias, and wrong self-assessments. Particularly, as we consider a potentially sensitive topic participants might have exag-

gerated their willingness to use protection mechanisms. Thus, claims regarding usage intentions should be interpreted with caution. Second, we included owners of different kinds of IoT devices instead of focusing on one specific device set, e.g., smart speakers. This probably caused variance in our data based on different device characteristics, such as subjective sensitivity of the collected information. However, we intended to gather a rich set of qualitative data to gain a deeper understanding of host considerations. We thus decided to include different kinds of IoT devices to be able to capture their views on the subject even if this included additional variance, as it also allowed us to gain insights on, for example, device-specific factors that influence IoT device owners' beliefs. Third, we used various guest privacy protection mechanisms for IoT-equipped environments from the literature to capture general considerations and requirements towards such protection mechanisms for guest privacy. Other examples of privacy protection mechanisms might reveal further essential aspects; hence, our results are to be understood as a first step towards understanding this complex topic. Finally, there are several limitations connected to our sample based on age, gender distribution. Because of that, our sample likely does not reflect the overall population of IoT device owners. Due to the lack of compensation, our sample may be biased towards those interested in research (higher education, etc.). Our final sample was between 23 and 43 years old, which matches the main population of IoT devices owners in 2020 [9]. During the recruitment, we invited all age groups above 18 years. Before participation, participants were screened based on whether or not they owned smart home devices. Most older participants that answered our screening could not participate since they did not match the target group of device owners.

4 Host Perspective Results

In this section, we present the interview results. Where appropriate, we include frequencies to give the reader an impression of how often the respective topic came up during the interviews. However, due to the qualitative and exploratory nature of our study, these frequencies should not be considered representative of the general population of IoT device owners.

4.1 RQ1: User Expectations

First, we wanted to understand how hosts expect privacy protection mechanisms for guests to be designed for broad adoption. Thus, when we interviewed IoT device owners about specific privacy protection mechanisms we asked them to explain why they would (not) use the respective mechanism. From these statements, we derived themes of requirements aiming to increase guest privacy in IoT-equipped environments.

4.1.1 No New Threats through Mechanisms

Obviously, privacy protection mechanisms should not pose a threat to the privacy of hosts or guests, ideally offering **privacy by default**. Consequently, 18 participants mentioned aspects related to this topic. Six of them described that guests should not have to provide additional data, like contact information, for protection mechanisms. This was mentioned in connection with mechanisms that delete guest data after a certain period of time and inform guests about that. Six participants stated that protection mechanisms should ensure IoT devices do not collect any data from guests without consent. Seven participants feared for their own privacy if protection mechanisms collected information about them (e.g., if and when they had guests in connection with filter mechanisms) or shared information with others (e.g., IoT devices at home). The latter was specially mentioned for mechanisms that send notifications to people who come near their apartments: "*I make myself too transparent for people who just walk by the outside of the apartment.*" (P16). Some participants also stated that they would not like guests to know about all IoT devices, e.g., security cameras. Further, six participants stated guests could adjust privacy settings using privacy protection mechanisms, as long as they were only allowed to employ stricter settings. These participants mainly feared guests could weaken privacy settings to enable additional functionalities of IoT devices which would be something they would feel very uncomfortable with: "*So maybe the guest comes and then suddenly says: okay, collect all data, which is a setting I have not set, then it's a breach of MY privacy. So the guest should not have that kind of control.*" (P7).

Few participants mentioned **cybersecurity** concerns. Three worried that protection mechanisms could induce security risks. One participant was afraid that protection mechanisms could provide opportunities to attack guests if the mechanism includes an app or send

notifications to the guest's phone: "*I can easily get much information about your phone, and if I want to do something malicious with it, I can somehow do it, because you are freely providing me data with your phone.*" (P7).

4.1.2 Required Resources Should be Low

Not surprisingly, **effortlessness** was among the essential characteristics a privacy protection mechanism for guests ought to have. Most participants repeatedly emphasized that such mechanisms should generate as little effort as possible for themselves (mentioned by N=17) or for their guests (mentioned by N=13). This included not only the continued use of mechanisms but also the initial setup: "*I buy IoT devices because they are convenient [...] I want to plug it in, and I want it to work. I don't want to spend forever messing with it.*" (P14). Accordingly, most participants mentioned that automation should be offered whenever possible to reduce workload.

A third of participants also mentioned that privacy protection mechanisms should be **easy to use**, i.e., operation of the mechanism should be self-explaining and intuitive. In this context, several participants referred to often complicated privacy settings menus as cautionary examples. This finding has also been found in studies that investigated IoT devices in general [39].

Some participants (N=5) expressed concerns about their guests being "*bombarded*" (P7) with notifications, especially regarding the concept of informing guests about the presence of IoT devices or the deletion of their data after a visit automatically. Hence, the mechanism should be **unintrusive**.

4.1.3 Privacy Should not Limit Hosts

Control by hosts was an essential aspect for most participants in the scope of all mechanisms in which guests could change privacy settings. This is a result related to findings on control over personal data in general repeatedly shown by related work [15, 33, 49]. Seventeen participants indicated that they would like to remain in charge of the IoT device, including privacy settings. For example, P13 said: "*What's nice about smart homes is that you feel like you're the only person who can adjust the devices. And, if you give that special measure to somebody else, I don't feel comfortable with that.*" In line with previous work [12], some participants feared that guests would disable functionalities they would like to keep enabled. Others were concerned that guests might weaken their privacy settings or alter the device settings to something they would not like. Most participants explained that they would feel uncomfortable if they were not informed about settings changes by guests.

Another finding that confirms related work [12] is that about half of our participants (N=9) were unwilling to **limit core functionalities** of IoT devices even temporarily to protect their guests' privacy. For instance, P14 said: "*Basically, these are all devices that serve some purpose and that I would like to use, even if my guest is there. [...] and if he then cuts the Internet connection of Alexa and I can no longer do voice control and cannot set an alarm clock in the kitchen, then that would really annoy me.*" Four of these participants also worried that privacy protection mechanisms could accidentally mess with the functionality of IoT devices.

Further, five participants stated that privacy protection mechanisms should be **appropriate** for the kind of guest data collected by the IoT device. E.g., IoT devices that do not collect sensitive guest data, either because of the device's functionality or because the guest would not use the room in which the IoT device is placed, should be excluded from the privacy protection mechanisms.

4.1.4 Mechanisms Should be Available for Guests

Six participants mentioned that their guests should **voluntarily** decide whether they would like to use privacy protection mechanisms. In this context, they referred to unobtrusive solutions, like dashboards or personal privacy assistance, instead of, e.g., informing guests verbally: "*Because it's not as intrusive as telling everyone. Anyone who cares can look at the dashboard and see what's installed, and anyone who doesn't care can ignore it.*" (P21).

Financial cost of privacy protection was also important. Some participants (N=4) stated that they were only willing to use privacy protection mechanisms that are free of charge, e.g., because do not want to buy equipment. This was particularly mentioned in connection with the information dashboard.

Ten participants said privacy protection mechanisms should serve as a mediator between hosts and guests. They should convey to the guest that the host consents to using the mechanism and potential changes to privacy settings: "*In some way, a signal to the guest that I don't have a problem with it and that no conflict will arise from them addressing that they have privacy concerns.*" (P16). Ideally, according to some participants, privacy protection mechanisms would be widely

known and thus **socially accepted**: "*I'll put it in guest mode, maybe it'll light up in a certain color, maybe because somehow word got around that 'okay, blue light means guest mode.' I'd like that.*" (P12).

Two participants would like privacy protection mechanisms to be **customizable** in the sense that guests can specify a profile and choose, e.g., about what kind of IoT devices they want to be notified. This feature was mainly associated with personal privacy assistants and notification functions, whereas static solutions like status indicators or dashboards were not expected to be customizable.

4.1.5 Mechanisms Should Be Salient and Aesthetic

Privacy protection mechanisms can only be useful if guests notice them. Hence, nine participants stated that mechanisms should be **salient**. While some participants were concerned that mechanisms integrated into the devices, e.g., status indicators or QR codes, would not suffice this purpose, others feared that conspicuous privacy protection mechanisms would conflict with **aesthetic** requirements: "*I guess that the dashboard isn't the most aesthetically pleasing, but if it is, it fades nicely into the background, which in turn defeats the purpose.*" (P14).

Five participants expressed that privacy protection mechanisms should even offer a function that allows guests to check settings to provide **assurance**. Assurance has already been identified as important factor by related work since devices might simply continue recording [1]. Suggested solutions for this include physical status indicators and the opportunity for guests to adjust or view settings: "*The risk here is that my guests must then rely on me to act in their interests, and I can imagine that the feeling of security is higher when the guests adjust the settings themselves.*" (P19).

In contrast to salience and assurance, more than a third of our participants (N=8) were only willing to use privacy protection mechanisms they find **aesthetic**, since the mechanisms would be part of their interior design. Similar aesthetic-related aspects were reported by related work that investigated early IoT devices [10] confirmed multiple times later on [1, 43, 48]. Some feared that the mechanism could destroy the IoT device's design, especially if the mechanism would include QR codes, e.g.: "*[...] because I think the devices are well designed and quite fashionable, and a QR code would disturb the whole thing a bit.*" (P11). Similar statements were given about dashboards and indicator lights.

4.1.6 Limitation to Guest Visit

Finally, five participants stated that changes made to their privacy settings should only be temporarily and ideally be reset automatically after the visit referring to **reversibility**. This feature was primarily associated with the guest mode concept.

4.2 RQ2: Impact Factors and Reasons

Second, we wanted to understand why hosts would use privacy protection mechanisms and which factors impact their decision to offer such mechanisms.

Reasons for Usage: Our participants described five reasons for using privacy protection mechanisms. Eight participants said they would employ privacy protection mechanisms so their **guests could feel comfortable** during the visit. Those participants said that a guest should feel safe in their homes, including "*that he does not feel observed or spied on*" (P11).

Also, eight participants believed that **guests should have the right to make their own decisions** about collecting their data. For example, P19 said: "*[...] because the moment a guest enters my home, I'm no longer the only one affected by the privacy settings, and so I could make sure that all affected people have control over how their data is handled.*"

Six participants stated that they want to be **open and transparent with guests** regarding the collection of data. Consequently, not telling guests about the potential collection of data was considered "*unfair*" (P18).

Four participants said they want to use protection mechanisms for guests due to **their own privacy values**. Still, two of those participants wanted to provide a privacy-friendly environment for their guests, while the other two mainly liked the thought of implementing privacy protection for their benefit.

Finally, three participants mentioned non-privacy-related reasons for implementing privacy protection mechanisms, describing that such mechanisms **do not impact their IoT device** user profile based on their guests' data.

Factors that Impact Usage: We further extracted four factors that influence the hosts' willingness to use privacy protection mechanisms for guests.

The first factor is the **type of collected data**. The type of sensor implemented in their IoT devices was a crucial factor for eight participants regarding their

willingness to use privacy protection mechanisms. While cameras and microphones were often referred as privacy-sensitive, vacuum robots were considered less privacy-invasive. Hence, owners of such IoT devices were less likely to employ protection mechanisms.

Some participants (N=5) also considered the **scope of the IoT device** distinguishing between those IoT devices they use for convenience and those they use for security purposes. Similar findings are reported in related work considering that perceptions can be guided by the primary functions of devices instead of the integrated sensors [1, 10]. Those participants were usually willing to limit their IoT device's functionality during visits to protect their guests' privacy if they used the IoT device for convenience, but not if they used it for security. The only IoT devices participants described to use due to security purposes were security cameras, e.g.: "*I'm often willing to sacrifice my own comfort for the benefit of my guests for the time of the visit, but if I put a camera on my front door, I put it there for a purpose. And the purpose is to record what's going on. Even if there is a guest coming at that moment or not.*" (P16).

Although our interview scenario explicitly referred to guests who were close to the interview participants, five participants emphasized that they were more willing to employ mechanisms that would protect the privacy of a very close friend or relative compared to other guests considering the **relationship to the guest**. This includes mechanisms aiming to inform guests about the presence of IoT devices; for example, P5 stated that he would not like anyone but close friends to know about his security cameras.

Some participants (N=6) referred to their own **privacy attitude**. Participants who valued their privacy were more willing to deploy privacy protection mechanisms for their guests, while participants who reported not being worried too much about privacy were less favorable to such mechanisms. However, P20 explicitly stated that she would like to implement privacy protection mechanisms for her guests since privacy was a topic she is usually not very aware of.

4.3 RQ3: Perceived Responsibilities

Third, we wanted to understand perceptions about the responsibility for guest privacy. When asked about who should be responsible for the guest's privacy, eleven participants saw hosts as responsible since they would know which devices are present. Please note that the reported numbers do not sum up to 100%, as some participants were ambivalent in their opinion and expressed several points of views during the interview. E.g., P19 said: "*As the person who introduced this smart home device into the situation, I am responsible for ensuring that my guests can be sure of their privacy.*" Still, seven participants said the guests should be responsible, and guests who were concerned about their privacy should communicate these concerns to the host and propose solutions. These participants said as they cannot know about the guest's privacy preferences, the guest should be "*the one who has to make sure that his needs are addressed*" (P11). Five participants thought that the host and the guest share responsibility, i.e., guests should communicate their wishes, and hosts should make sure that these are fulfilled. For example, P21 said: "*Since I as a host cannot guess the needs of the guest it would be at least on the guest to express what would be important or whether there are concerns. But that this is then implemented, that can lie on the host side.*" This finding is connected to the cooperative mechanisms from Yao et al. [49] and Cobb et al. [12]. Two participants placed the responsibility neither on guests nor hosts but on the device manufacturers since those were in charge of deciding on the data collection functionalities. A few participants also mentioned the social implications of using privacy protection mechanisms for their guests.

Some (N=4) participants said that it would be awkward for them if their guests would try to change (privacy) settings of their IoT devices. They explained that they have the **right to set the rules in their home**, and guests should submit to these rules. Guests adjusting the settings of their IoT devices was considered similar to "*changing the decoration because a guest does not like it*" (P15) or changing the window settings (P20). Two participants also stated that guests should adjust their privacy attitude to that of the host if they were visiting someone: "*So that's simply an expectation that I have of them, that they're not data protection fascists to put it a bit exaggeratedly, but that they also adapt to my values and so on in my apartment.*" (P14).

Three participants stated that no additional privacy protection mechanisms should be necessary for guests since guests should **trust hosts** which relates to findings about child privacy [10]. These participants said they would be offended if a guest would try to check an IoT device's privacy settings or the kind of collected data, e.g., via QR codes, as this would be a "*sign of mistrust*" (P8), and they would expect guests they are close to feeling comfortable and safe in their home, without additional proof or measures.

Yet, four participants were concerned that the privacy protection mechanisms would result in their guests **not receiving a warm welcome**. They thought that informing their guests about their IoT devices or adjusting its settings during the welcome would feel "*mechanical*" (P12), "*overwhelming and socially weird*" (P15), or "*unpleasant and bureaucratic*" (P8).

Only three participants explained that they would **not take it personally** if guests would like to adjust or check their IoT device settings. For example, P7 said: "*They have issues with my device, not issues with me, so I would not mind at all if they were direct with me 'I'm not comfortable with it, can you just turn it off?"'*

4.4 RQ4: Device Disclosure

Forth, we aimed to comprehend how and why hosts disclose devices to their guests and how guests react to that. When asked directly whether they inform their guests about IoT devices, 13 participants said they never notify guests, five stated to always inform their guests, and three said that they only sometimes inform their guests.

Still, during the interviews, 14 participants reported informing their guests about IoT devices under **certain circumstances**. Most of these participants said they would only inform guests if they know that privacy is important to them. Some participants also limited disclose to IoT devices that collect data they consider to be sensitive, such as voice and pictures confirming a finding by Choe et al. [10]. Again, others said that they would only tell their guests about IoT devices if the guests had already spotted the devices.

Half of participants gave **reasons for not telling** their guests about IoT devices. Most explained not wanting their guests to consider their home dangerous. Some feared guests who are not concerned about IoT devices would begin to worry about their privacy if they explicitly made them aware of the IoT devices, with "*neutral guests*" becoming "*sensitive guests*" (P8). Other reasons for not informing guests include the process of informing them being too cumbersome (N=1), hosts thought they should not have to justify themselves for their own home (N=2), so far, even if guests had found out about the IoT devices after the visit, no one complained about not being made aware of the devices (N=3), the IoT devices do not affect guests as they do not collect sensitive data or do not operate when guests are present (N=5), because it "*has become so normal to own such a device*" (P11).

When asked about **how devices are disclosed**, sixteen participants said to have shown their IoT devices to their guests at some point during the visit. However, most of them only wanted to demonstrate the device's functionalities without mentioning privacy or data collection issues. Our participants mainly reported to mention IoT devices if they came up naturally during the conversation or at the moment they operate the devices: "*When it [the door] unlocks automatically and then swings open on its own, and those are the moments when I get to talk.*" (P14). Only one participant reported having informed his guests about his IoT devices in terms of data collection. In particular, he described making jokes about his security cameras: "*I always joke that I'll give them my privacy policy to sign because there are cameras.*" (P3). Yet, he also reported to demonstrate the data collected to guests who are critical by showing "*how wide the angle is, i.e. up to where you can be seen and from where no longer*" (P3).

When asked about **guest reactions**, most participants (N=18) talked about how guests who noticed their devices reacted to them. However, only three reported negative reactions. Mainly, our participants said that their guests had either no reaction since they were already familiar with IoT devices (e.g., Amazon Echo) or own devices themselves; or their guests had shown positive interest, being enthusiastic about device functionality. The negative reactions included guests having "*doubts*" (P10), being "*still a bit unfamiliar with it*" (P21), and one guest being "*overwhelmed*" and explaining that they "*don't like being listened to*" by the devices (P15). Still, our participants reported that no one asked them to turn off their IoT devices so far.

5 Study II: Guest Perspective

While our first study revealed the perspective of hosts, it remains unclear to which extent the wishes of hosts match those of guests and how guests evaluate impact factors, reasons, responsibility, and device disclosure. Hence, the goal for the second study was adding the guest perspective to our investigation. We, therefore, conducted a survey study with 264 participants. To investigate whether owning IoT devices impacts the guest perspective, the sample consisted of 115 IoT device owners and 149 non-owners. The survey items were developed based on the codes identified during the interview analysis.

	age	gender	ATI scale [17] mean	ATI scale [17] SD	IUIPC [30] mean	IUIPC [30] SD
owners	< 20: 3.5% 20-25: 4.3% 26-35: 7.8% 36-45: 19.1% 46-55: 38.3% 56-65: 27.0%	Male: 67.8% Female: 32.2% Other: 0.0%	4.19	0.65	Awareness: 5.91 Control: 5.74 Collection: 5.67	Awareness: 0.90 Control: 1.05 Collection: 1.07
non-owners	< 20: 5.4% 20-25: 10.1% 26-35: 12.1% 36-45: 24.2% 46-55: 29.5% 56-65: 18.8%	Male: 51.0% Female: 48.3% Other: 0.7%	4.22	0.66	Awareness: 5.96 Control: 5.94 Collection: 5.92	Awareness: 0.96 Control: 1.00 Collection: 1.08

Table 2. Demographics of the online study sample.

Procedure. The online study consisted of seven main parts. We further applied two simple attention check questions. First, participants were asked to give their informed consent. We then welcomed and thanked them for their participation. They were then introduced to the study scenario, which is a visit to a friend with IoT devices at their home.

Second, we gave a definition of an IoT device [3] and asked participants about their IoT devices.Third, we asked the participants to rate the importance of the user expectations that we captured from the interview results on a 5-point Likert scale. Fourth, we asked if and how the participants had been made aware of IoT devices when visiting IoT-equipped households, how they reacted in that situation, and whether they would like to be informed when visiting an IoT-equipped household. We used several multiple-choice and open-answer questions, which were partly implemented as filter questions. Fifth, we asked who the participants thought was responsible for guest privacy using a multiple-choice question. Sixth, we asked the participants to rate the various reasons for using privacy protection mechanisms for guests identified in the interviews using a 5-point Likert scale. Seventh, we focused on the social aspects of providing and using privacy protection mechanisms for guests identified in the interviews, again by using a 5-point Likert scale. Finally, we asked for demographics using several multiple choice and open questions, the IUIPC [30] and Affinity of Technology (ATI) scales [17]. We then thanked the participants and redirected them to Prolific. This procedure meets all requirements proposed by our university's ethics commission.

Participants. We recruited two samples using the online recruitment platform Prolific. They were reimbursed with an hourly rate of 9£.The participants were located in different countries, including the UK, US, Canada, Germany, France, and further European countries. Participants in the first sample were required to own IoT devices with audio or video recording capabilities, while participants in the second sample were required not to own such devices. Sixteen participants in the non-owner group reported owning IoT devices with audio or video recording capabilities, and 37 vice-versa. Thus, we re-assigned the respective participants based on that information. The participants were reimbursed, matching an hourly rate of nine pounds. A total of 289 participants completed the survey; demographics are given in Table 2. Twenty-five failed at least one of the attention checks and were excluded for analysis. Thus, the final sample includes 264 participants, of which 115 owned IoT devices meeting our criteria.

Data Analysis. To analyze our survey results, we first tested whether our data is normal-distributed. Since normal distribution was not given for any of the Likert items, we calculated descriptive statistics including the mean, median and percentiles (25 and 75). To analyze multiple-choice items, we applied Pearson's χ^2 tests. Free-text answers were analyzed using thematic analysis. One author coded all answers. A second researcher verified the coding, and disagreements were discussed.

Limitations. Like most survey studies, our survey study has several limitations. First, we rely on self-reported data. However, it may be challenging for participants to make judgements on, e.g., importance of

user wishes for potential privacy protection mechanisms without actually interacting with such mechanisms in a genuine visit scenario. Second, we build on the interview results, as the goal of the online survey was extending the interview results by the guest perspective. Hence, we only considered factors that came up during the interviews. Another study design using more open-ended questions might have led to other results.Third, our participants self-described as rather tech-savvy and privacy-aware. Since we relied on Prolific for recruitment, which is located in the UK, our sample included mainly participants from western cultures. Participants from other, more collectivist cultures might have expressed different beliefs, e.g., regarding social aspects. Thus, our survey results can only serve as a first step towards understanding users' needs and expectations towards privacy protection mechanisms for guests in IoT-equipped environments and should be validated through future in-depth studies in the field with a more heterogeneous sample.

6 Guest Perspective Results

In this section, we report the results of the guest perspective. Overall, the guests rated all requirements as either neutral, rather important or important. Thus, they likely are not in conflict with the host perspective. Figure 1a) also depicts the survey results.

6.1 RQ1: User Expectations

In this section, we report the results of the guest perspective regarding individual user expectations. For this, we provide a descriptive analysis of the answers to the Likert items below. For the detailed descriptive statistics including the mean, median and percentiles (Q1 and Q3), we refer the reader to Appendix B. Overall, we could only observe few differences between the perspectives of guests that own IoT devices and those who do not. Below, we report and discuss the results grouped by their ratings. Except for aspects that are not specifically connected to the guest or their visit, all requirements were considered to be important.

6.1.1 Aspects Unrelated to Guests are Neutral.

The requirements *aesthetics*, *reversibility*, and *little effort for hosts* were rated similarly neutral by owners and non-owners in the guest group (Md=3.00 respectively; 1=very unimportant, 5=very important). These requirements share that the user wishes affect someone other than the guest, or are not connected to the visit. In particular, *aesthetics*, consider the living space of other individuals *while little effort for hosts* does not affect guests. Reversibility does not affect the visit of the guest because it refers to an action after it.

6.1.2 Importantly Rated Requirements Consider Guests and the Social Level

All requirements reported below, unless specifically stated, were rated as important (Md=4.00) by both non-owners and owners of IoT devices in the guest perspective. We report the requirements in sets of overall themes to facilitate discussion.

Resources Should be Kept Low. The requirements *little effort for guests* and *scalability* share a connection to required resources for privacy protection. That matches several investigations from related work (cf. [13]). Considering *ease-of-use*, owners and non-owners rated importance differently. Owners of IoT devices considered it as neutral (Md=3.00), while non-owners considered it important (Md=4.00). This difference might be rooted in that owners are more familiar with IoT devices which might lower the barrier of interacting with them, while non-owners might require more support. Further perceptions regarding *free of charge* differed. While owners considered it important (Md=4.00), non-owners considered it very important (Md=5.00) showing that the cost of privacy protection is essential. Finally, *salience* meaning that the privacy mechanism should be clearly visible and *assurance* were considered to be similarly important adding to the overall scheme, that the resources for guest privacy protection should be low.

No Impact and Host Control. The evaluations of the requirements *no impact on the functionality* and that *hosts keep control* underline that privacy protection of guests is a rather secondary goal during a visit. Further, these results do not reveal any tensions between guests that own IoT device and those who do not. Further, *no weakening of privacy settings* was also considered to be important showing that guests do not want to interfere with the host's privacy preferences.

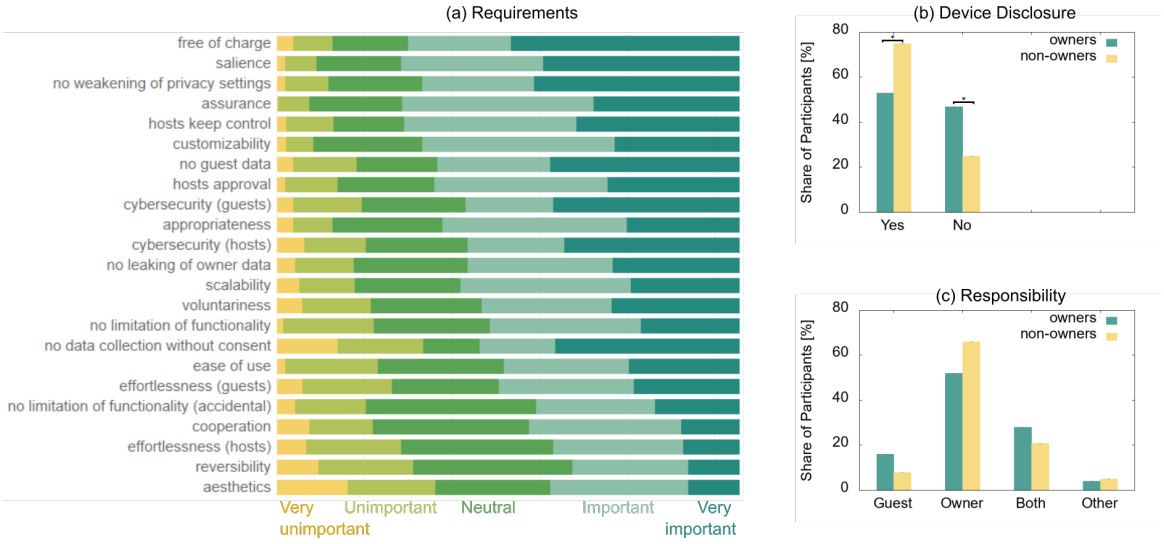

Fig. 1. Results from the online survey. The Likert statements are given in Appendix B

Privacy and Cybersecurity Aspects. Overall, participants in the perspective of non-owners and owners agreed about the importance of *no cybersecurity risks for hosts*, *no cybersecurity risks for guests*. Similar assessments were given to privacy related aspects, namely *no information leakage about the host* and the guests' wish not to *provide data for mechanisms*, such as contact information.

Participants in the guest perspective furthermore agreed that a privacy mechanism should not allow them to *weaken privacy settings of hosts* (Md=4.00 respectively) and that the mechanism should only affect devices that *collect sensitive data* and capture data only after the *guest's consent*.

Importance of the Social Level. Being able to use the mechanisms *voluntarily* was considered similarly to *social acceptability* by hosts. This shows that even if privacy is a rather secondary goal during a visit, social aspects are still considered to be important when it comes to privacy protection for guests. Yet, participants considered the importance of *cooperation of hosts and guests* as neutral (Md=3.00 respectively) indicating mechanisms should rather be designed for individual usage which is a contrasting result to related work [12, 48]. This is also underlined by the ratings regarding the requirement of *individually adjustable* mechanisms which was considered to be important (Md=4.00 respectively).

6.2 RQ2: Impact Factors & Usage

To investigate impact factors, we presented four statements to the participants. In contrast to the user wishes above, we found fewer agreements between owners and non-owners of IoT devices in the guest perspective.

The importance of the statement *guest should adjust to the owner's privacy preferences* was rated to be neutral (Md=3.00 respectively). *The focus should be on the purpose of the visit and not on privacy protection* as well as *that the IoT device owner should not take guest privacy wishes personally* were again agreed on (Md=4.00 respectively) which supports the user wished from the social level detailed above. The statement *"The guest should trust the host"* was perceived as important by the owners (Md=4.00) and neutral by the non-owners (Md=3.00).

Considering the reasons for using privacy protection mechanisms, non-owners and owners agreed regarding *guest comfort* and *the guests' right for privacy* (Md=5.00 respectively). Further, both groups agreed that reasons for usage are that *the host values privacy*, *the host is aware of privacy issues*, and that *profile of the host is not impacted by data from the guest* (Md=4.00 respectively).

Opinions about the importance of *transparency towards the guest* differed. While owners considered it to be important (Md=4.00), the non-owners considered to be very important (Md=5.00).

6.3 RQ3: Responsibility

When we asked the participants about who is responsible for guest privacy protection, the views differed slightly among owners and non-owners (see Figure 1c). A Pearson's χ^2-test was performed to examine the relationship between the ownership of devices and the responsibility. The relation between these variables was significant ($\chi^2(3) = 9.57$, $p = .032$, $Cramer's\ V = .19$). However, pairwise comparisons did not reveal significant differences. We applied Bonferroni correction to prevent inflation of type I errors (corrected α-level = 0.0167). The p-values from these tests are as follows: owners and both received $\chi^2(1) = 4.86$, $p = .027$, owners and guests $\chi^2(1) = 3.72$, $p = .054$, and guests against both $\chi^2(1) = 0.10$, $p = .748$.

6.4 RQ4: Device Disclosure

We also asked our participants whether they want to be informed about IoT devices when visiting a friend. 53.0% of the participants that owned IoT devices (N=61) answered this question affirmatively, and 75.2% (N=112) of the participants without IoT devices did (see also Figure 1b). A Pearson χ^2-test was performed to examine the relationship between the ownership of devices and the wish for device disclosure and revealed significant results ($\chi^2(1) = 14.1$, $p < .001$, $Cramer's\ V = .231$). Depending on their answers, we asked the participants either why they do not want to be informed about IoT devices or why and how they would like to be informed. Here, the participants could provide free-text answers.

Those participants that wanted to be informed named[1] awareness (N=72), privacy-related reasons (N=39), and general interest in IoT devices (N=51) as reasons. When asked how they want to be informed, they named verbally by the owner (N=123), by signs (N=6), by notifications (N=33), and by other platforms (N=8), such as the media or social networks, as possibilities for device disclosure. Of them, 18 participants mentioned that the device disclosure should be before entering the household. Those who do not want to be informed named the following reasons: general disinterest (N=23), no concern about IoT devices (N=29), too much effort (N=6), or trust in the owner (N=6). Further, seven participants questioned the effectiveness of privacy protection because there is no way to escape, nine considered that they do not have to be informed based on their role as a guest. Four considered the purpose of the visit to be more important. When asked whether there attention was drawn to IoT devices, 55.2% of device owners and 37.9% answered this question affirmatively. A Pearson χ^2-test revealed significant results ($\chi^2(1) = 7.12$, $p = .008$, $Cramer's\ V = .164$).

1 The reported numbers do not sum up to the number of participants, as some participants provided unclear statements.

7 Discussion

In this section, we discuss the *investigated mechanisms*, *owners versus hosts,* and *device disclosure responsibility*. Based on that, we identify a *design space* for guest privacy protection.

7.1 Investigated Mechanisms

In the host study, we investigated four categories of privacy protection mechanisms with a total of ten specific mechanisms. Overall, we can conclude that there is no one-size-fits-all solution that serves each and every host because each mechanism has individual benefits and drawbacks. This is also reflected in overall set of requirements that we identified. While each individual requirement is sound, there are some requirements that conflict with each other.

Provider Support is Needed. Benefits, drawbacks as well as the fulfilment of requirements by the individual mechanisms is challenging to determine because it is connected to a specific implementation. The requirements *reversibility*, *appropriateness*, *privacy by default*, *cybersecurity*, *host control* could be integrated into each investigated mechanism if the provider of the IoT device implements the required functionality. The *cost* of privacy protection mechanisms in terms of financial resources is also largely dependent on providers.

Salience Interferes with Aesthetics. The requirement *aesthetics* considers visual aspects of the living space. Hence, it is highly individual and depends on hosts. The mechanisms' status and location indicators, device labels (e.g., QR codes), dashboard, and the visual representation of the guest mode can be affected by this requirement. All other mechanisms do not alter the visual aspects of the living space. There is a

tension between salience and aesthetics since the visibility of a mechanism might impact a living space. While the importance of *aesthetics* were rated neutral in the guest perspective, it was important for the hosts. Participants, especially in the guest perspective, considered the salience, i.e. the visibility of the mechanism, as important confirming previous studies of guest privacy [33, 49]. Hosts, in general, do not want to be restricted by privacy protection when decorating their living space, while guests might place a stronger focus on privacy aspects. A similar tension between aesthetics and salience was reported in an early investigation of home sensing technologies [10]. Similar results have been demonstrated in life-logging studies [24].

Involvement Impacts Effort. *Effortlessness for hosts* is difficult to assure in mechanisms that require host actions. Status and location indicators, device labels, and the dashboard only have to be set up once. Verbal device disclosure, settings access, guest modes, and cooperation might have to be used multiple times during visits, drawing effortlessness for hosts into question. This aspect is similar for *effortlessness* that considers *guests*, however, other mechanisms are also affected. Personal privacy assistance ideally has to be set up only once, or learns guest preferences automatically. Notifications, status and location indicators and the dashboard might trigger guests to multiple actions. This is similar to device labels which have to be searched and interpreted by the guests. Guest modes, setting access, and cooperation also require the guests to act multiple times, drawing effortlessness into question. *Unintrusiveness* means that guests should not receive too many notifications from privacy protection mechanisms. Depending on the number of IoT devices, the notification mechanism might not fulfil this requirement. This is similar to the data deletion if the guests get notified about each IoT device. Personal privacy assistance can come in various configurations [13]. If privacy assistance is based on notifications without further automation, it is identical to a simple notification mechanism from the unintrusiveness point of view.

Customizability is Challenging. *Customizability* means that guests can configure the privacy protection mechanism matching their preferences. This aspect is not given for everything that is exclusively configured and installed by hosts: status and location indication, device labels, and dashboards. Further, verbal device disclosure is an action by the host. *Customizability* is offered by notifications, guest mode, settings access, cooperation, and personal privacy assistance.

7.2 Social Level

Responsibility. The topic of responsibility is a complex subject. In general, more than half of participants in the interview study considered the owner to be responsible for the guest privacy protection. Considering the online study that investigated the guest's perspective, there was a tendency that the owner is responsible. This seems reasonable since the host is also responsible for their IoT devices and -in contrast to the guest- is easily aware. However, this strengthens the existing power imbalance between owners and guests since the guests would rely on the owner to inform them about (non-obvious) devices. If guests do not know about devices, it might be challenging or even impossible to take matters into their own hands.

Related work showed that not only the parties that our participants named are considered when it comes to responsibility. As such, manufacturers and even the government play a role in privacy protection [20]. Considering the government, several countries already have privacy regulations in place, such as the General Data Protection Regulation (GDPR) from the European Union. There, it is stated in Article 6 that personal data may not be processed unless "the data subject has given consent to the processing of his or her personal data for one or more specific purposes" [40] meaning guests have to be informed somehow to give consent.

Filtering guest data would not require consent because no personal data is captured. However, the privacy of guests might still be affected if filtering is not processed on the respective IoT device. Informing guests such that they can give their consent requires cooperation either from the manufacturer, the host, or both. Manufacturers could implement APIs for privacy assistance or notification mechanisms. Guests could then configure and use these mechanisms on their personal devices. In this scenario, a cooperation from hosts is not needed. For this, however, guests have to know about privacy assistance or notification mechanisms, which might be challenging.

If none of the mechanisms mentioned above is used, guests still need to know about IoT devices to give their consent. As stated by some of our participants and in related work, guests might be unaware of IoT devices, and even if they know about them, they might not know about the device's data capturing capabilities [49]. Con-

sequently, the hosts are the only party that up to now can really ensure that guests know about devices.

Tensions between Hosts and Guests. When investigating the different mechanisms, we asked questions about the social level. While there seems to be a tendency for hosts to accommodate the wishes of guests, there are also tensions. Some hosts saw privacy protection as a violation of their own home and compared it to physical changes in the living space. Consequently, differences in privacy attitudes might result in conflicts between hosts and guests. While we do not wish to speculate on further impacts on the social level, we argue that mechanisms that require no guest interaction, such as filters, might be a viable solution here since they do not require privacy aspects to be communicated.

Another tension point was related to the weakening of host settings and loss of functionality. Consequently, a mechanism should only allow guests to impose stronger privacy settings which was also welcomed from the guest perspective. Loss of functionality might be more challenging to address, because guests might want devices to be switched off that deliver additional comfort. Participants in the host perspective stated not wanting to sacrifice functionality for guest privacy. This again would demand IoT devices that can offer their benefits without capturing guest data. Data recipients and processing locations have been identified by related work as an impact factor when it comes to privacy decisions. Hence, located data processing on the device or within the IoT-equipped environment might address these issues.

7.3 Proposed Design Space

Based on the results of our investigation and related work, we propose a design space for guest privacy protection in IoT-equipped environments. Our design space consists of nine dimensions (see also Fig. 2).

Required Data. The first dimension considers the data needed for guest privacy protection, because the data required for the mechanism to be effective is important for implementation. The first kind of data is the *information displayed to guests*. This starts with disclosure of the IoT device itself and finishes with sensor information that might be a threat to the host's privacy. The second kind of data is *information provided by the guest*. For instance, a mechanism requires contact information if guests are notified about successful data deletion after a visit.

Scope of Privacy Protection. The scope of the mechanism forms the second dimension of the design space. A privacy protection mechanism can be located on each *individual device* (e.g., labels) or a solution that considers *multiple or even all IoT devices* (e.g., privacy assistance). The scope of privacy protection impacts how hosts disclose IoT devices and the resources required. Ideally, the scope should only cover devices that can capture privacy-sensitive data about guests. Further, the scope should ideally be limited to locations where guests have access to, referring to participant statements that they do not wish passersby outside their house to configure devices inside.

Effect. The next dimension is the effect on functionality. This could be the *entire device* meaning that devices cannot be used if the guests do not consent to the data processing. Second, only the *data collection function*, e.g., the camera function of a smart fridge, could be affected. This is also co-motivated by related work [12].

User Involvement. The degree of user involvement was considered as crucial by many participants but also in related work [12, 13, 43, 49]. Consequently, it forms the third dimension in our design space. Mechanisms can be configured *once during setup* and require no further maintenance resulting in minimal user involvement. Further, the involvement can be connected to *each visit*. The maximal user involvement is when guests or hosts need to interact with the mechanism whenever data is captured (*request-based*). A further way that impacts the user involvement is *reversibility* meaning that privacy settings automatically revert to the host's preferences once the guest has left.

Financial Burden. Next, the financial cost of privacy protection is important for individuals. Many of our participants explicitly stated guest privacy protection should even be *free of charge* for hosts and guests. However, there can also be *one-time* or *recurring costs*.

Burden on Social Aspects. The next dimension of our design space is burden on social aspects, meaning the degree to which the social situation is disrupted by configuring privacy mechanisms. Situations that impact social aspects have also been identified by related work [10, 49]. Compared to the burden on individuals, this also considers communication-related aspects between hosts and guests. There could be *no interaction* between hosts and guests in case of automatic mechanisms, such as filtering. No interaction would likely not

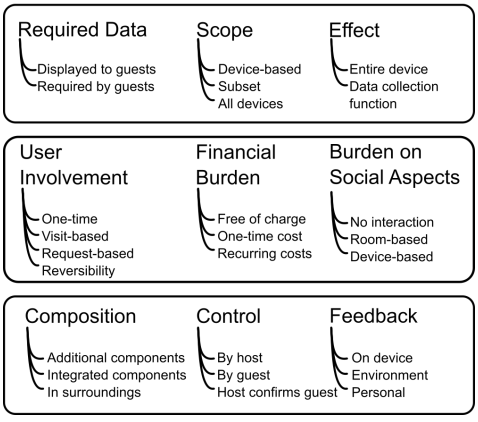

Fig. 2. Overview of the proposed design space.

impact the social level. The next level is based on the entire environment meaning that the host could introduce sensor functionality of the household as a whole. This is followed by room-based interaction meaning that the host introduces sensor functionality in each room. The final level is given by *device-based interaction* meaning that hosts and guests would have to interact with each other at least once per active device.

Composition. The composition of the mechanism refers to the degree it can be integrated into the hosts' living spaces without disrupting aesthetic aspects. Privacy protection mechanisms could be *additional components*, such as labels [49], that normally are not part of the living space. Second, they could be extra components that are *configurable* by the hosts in terms of design, such as colors. Finally, the mechanisms could be *integrated* into their surroundings or the devices to match the living space design.

Control. Control by hosts about their home was another integral aspect. This dimension refers to the entity that controls the privacy mechanism. It could be *fully host-controlled*, *fully guest-controlled*, or *hosts confirm guest choices*. This dimension is also co-motivated by related work that repeatedly identified the importance of control over data in several perspectives [15, 49–52].

Feedback. Feedback in terms of salience and assurance was essential for guests and has also been identified as important by related work [1, 33]. The feedback dimension refers to the information that guests receive about executing their privacy decision by the mechanism. There could be *on device feedback* meaning that the IoT device includes a feedback mechanism, e.g., status indicators. There could be feedback in the *environment* meaning that guests can obtain status information in their surroundings, e.g., via a dynamic dashboard. Finally, the feedback could be *personal*, i.e. visible to or hosts guests, for instance on their personal devices.

8 Conclusion and Future Work

In this paper, we presented an investigation of two perspectives on protection mechanisms for guests in IoT-equipped households. From our results, we derive requirements for guest privacy protection and use them to identify a design space. We learned that responsibility for guest privacy is a complex topic. Considering our participants, they tended to see the responsibility on the host's side. Due to the explorative nature of our study, our investigation serves as a stepping stone for enabling privacy protection for guests in IoT-equipped households. Based on our work, we consider several directions of future work as essential. First, we investigated visits of close friends, hence, future studies should expand this investigation to other types of guests. Personal privacy assistance might be a promising solution for guest privacy that fulfils many of our requirements. Privacy assistance might even be so automated that they act on the guest's behalf while keeping the privacy of the host. To fulfil this task, it is not required for the guest to know about IoT devices. However, this might impact verification options of the assistant's actions. Future work should investigate to which extent verification of the assistant's actions must be provided. Another direction for future work is given by the focus of our study investigating on privacy protection mechanisms as a whole without providing details, such as data recipients or storage duration. While these have been identified by related work as important decision factors [15], future work should investigate how to integrate this information into privacy protection mechanisms. Filter mechanisms that let IoT devices provide their usual functionality without processing any data of guests might be viable solutions that do not affect the social level. Further, mechanisms could in general be only activated if required, e.g., speakers could only capture data if they are intentionally spoken to [37]. However, this only applies if filtering is done on the IoT device. Hence, the development of filtering solutions forms a crucial task of future work.

Acknowledgements

This work has been co-funded by the German Federal Ministry of Education and Research (BMBF) within the SWC 2.0 "PrivacyGate" 01|S17050, by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation, grant number 251805230/GRK 2050) and by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

References

[1] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proc. of the ACM on Human-Computer Interaction (HCI)*, 4(CSCW2), October 2020.

[2] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. Discovering smart home internet of things privacy norms using contextual integrity. *Proc. of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 2(2):59, 2018.

[3] Luigi Atzori, Antonio Iera, and Giacomo Morabito. Understanding the internet of things: Definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, 56:122–140, 2017.

[4] Julia Bernd, Ruba Abu-Salma, and Alisa Frik. Bystanders' privacy: The perspectives of nannies on smart home surveillance. In *Proc. of the 10th USENIX Workshop on Free and Open Communications on the Internet*, FOCI. USENIX Association, 2020.

[5] BigBlueButton. Big blue button – engage your online students, 2021. https://bigbluebutton.org/ (Accessed 23-05-21).

[6] Denys Brand, Florence D. DiGennaro Reed, Mariah D. Morley, Tyler G. Erath, and Matthew D. Novak. A survey assessing privacy concerns of smart-home services provided to individuals with disabilities. *Behavior Analysis in Practice*, 13:11–21, 2019.

[7] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.

[8] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. On privacy and security challenges in smart connected homes. In *Proc. of the European Intelligence and Security Informatics Conference*, EISIC, pages 172–175. IEEE, 2016.

[9] Statistisches Bundesamt. Zahl der woche – 3,3 millionen menschen nutzten 2020 smarte haushaltsgeräte, 2021. https://www.destatis.de/DE/Presse/Pressemitteilungen/Zahl-der-Woche/2021/PD21_27_p002.html (Accessed 20-February-2022).

[10] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *Proc. of the Conference on Ubiquitous Computing*, UbiComp, pages 61–70, New York, NY, USA, 2012. ACM.

[11] Hyunji Chung, Michaela Iorga, Jeffrey Voas, and Sangjin Lee. Alexa, can I trust you? *Computer*, 50(9):100–104, 2017.

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

[13] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. Informing the design of a personalized privacy assistant for the internet of things. In *Proc. of the CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–13, New York, NY, USA, 2020. ACM.

[14] Anupam Das, Martin Degeling, Daniel Smullen, and Norman Sadeh. Personalized privacy assistants for the internet of things: Providing users with notice and choice. *IEEE Pervasive Computing*, 17(3):35–46, Jul 2018.

[15] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Cranor, and Norman Sadeh. Privacy expectations and preferences in an iot world. In *Proc. of the Symposium on Usable Privacy and Security*, SOUPS '17, pages 399–412, Berkeley, CA, USA, 2017. USENIX Association.

[16] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. A design space for privacy choices: Towards meaningful privacy control in the internet of things. In *Proc. of the CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. ACM.

[17] Thomas Franke, Christiane Attig, and Daniel Wessel. 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):456–467, 2019.

[18] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "a stalker's paradise": How intimate partner abusers exploit technology. In *Proc. of the CHI Conference on Human Factors in Computing Systems*, pages 1–13, New York, NY, USA, 2018. ACM.

[19] Christine Geeng and Franziska Roesner. Who's in control? interactions in multi-user smart homes. In *Proc. of the CHI Conference on Human Factors in Computing Systems*, CHI '19, pages 1–13, New York, NY, USA, 2019. ACM.

[20] Julie Haney, Yasemin Acar, and Susanne Furman. "it's the company, the government, you and I": User perceptions of responsibility for smart home privacy and security. In *Proc. of the 30th USENIX Security Symposium*, USENIX Security 21, Vancouver, B.C., 2021. USENIX Association.

[21] Julie M. Haney, Susanne M. Furman, and Yasemin Acar. Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. In *Proc. of the International Conference on Human-Computer Interaction*, pages 393–411, Cham, Switzerland, 2020. Springer.

[22] Rakibul Hasan, David Crandall, Mario Fritz, and Apu Kapadia. Automatically detecting bystanders in photos to reduce privacy risks. In *Proc. of the IEEE Symposium on Security*

and Privacy, S&P, pages 318–335, 2020.

[23] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. Rethinking access control and authentication for the home internet of things (IoT). In *Proc. of the 27th USENIX Security Symposium*, USENIX Security 18, pages 255–272, Baltimore, MD, 2018. USENIX Association.

[24] Marion Koelle, Matthias Kranz, and Andreas Möller. Don't look at me that way!: Understanding user attitudes towards data glasses usage. In *Proc. of the International Conference on Human-Computer Interaction with Mobile Devices and Services*, MobileHCI '15, pages 362–372, New York, NY, USA, 2015. ACM.

[25] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. "we just use what they give us": Understanding passenger user perspectives in smart homes. In *Proc. of the CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[26] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 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):102, 2018.

[27] H. Lee and A. Kobsa. Understanding user privacy in internet of things environments. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pages 407–412, New York, NY, USA, 2016. IEEE.

[28] Yuchen Liu, Ziyu Xiang, Eun Ji Seong, Apu Kapadia, and Donald S. Williamson. Defending against microphone-based attacks with personalized noise. *Proc. on Privacy Enhancing Technologies*, 2021(2):130–150, 2021.

[29] Bojana Lobe, David Morgan, and Kim A. Hoffman. Qualitative data collection in an era of social distancing. *International Journal of Qualitative Methods*, 19:1609406920937875, 2020.

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

[31] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. Smart devices in airbnbs: Considering privacy and security for both guests and hosts. *Proc. on Privacy Enhancing Technologies*, 2020(2):436–458, 2020.

[32] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. "you just can't know about everything": Privacy perceptions of smart home visitors. In *Proc. of the 19th International Conference on Mobile and Ubiquitous Multimedia*, MUM, page 83–95, New York, NY, USA, 2020. ACM.

[33] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. "i don't know how to protect myself": Understanding privacy perceptions resulting from the presence of bystanders in smart environments. In *Proc. of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, NordiCHI '20, New York, NY, USA, 2020. ACM.

[34] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 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), November 2019.

[35] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. Toys that listen: A study of parents, children, and internet-connected toys. In *Proc. of the CHI Conference on Human Factors in Computing Systems*, CHI '17, page 5197–5207, New York, NY, USA, 2017. ACM.

[36] Sarah Mennicken, David Kim, and Elaine May Huang. Integrating the smart home into the digital calendar. In *Proc. of the CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 5958–5969, New York, NY, USA, 2016. ACM.

[37] Abraham Mhaidli, Manikandan Kandadai Venkatesh, Yixin Zou, and Florian Schaub. Listen only when spoken to: Interpersonal communication cues as smart speaker privacy controls. *Proc. on Privacy Enhancing Technologies*, 2020(2):251–270, 2020.

[38] Antti Oulasvirta, Aurora Pihlajamaa, Jukka Perkiö, Debarshi Ray, Taneli Vähäkangas, Tero Hasu, Niklas Vainio, and Petri Myllymäki. Long-term effects of ubiquitous surveillance in the home. In *Proc. of the ACM Conference on Ubiquitous Computing*, UbiComp '12, page 41–50, New York, NY, USA, 2012. ACM.

[39] Xinru Page, Paritosh Bahirat, Muhammad I. Safi, Bart P. Knijnenburg, and Pamela Wisniewski. The internet of what? understanding differences in perceptions and adoption for the internet of things. *Proc. of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 2(4), December 2018.

[40] European Parliament. Regulation (eu) 2016/679council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation), 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679 (Accessed 02-February-2021).

[41] Sarah Pidcock, Rob Smits, Urs Hengartner, and Ian Goldberg. Notisense: An urban sensing notification system to improve bystander privacy. In *Proc. of the International Workshop Sensing Applications on Mobile Phones*, PhoneSense '11, pages 1–5, 2011.

[42] James Pierce. Smart home security cameras and shifting lines of creepiness: A design-led inquiry. In *Proc. of the CHI Conference on Human Factors in Computing Systems*, CHI '19, pages 1—-14, New York, NY, USA, 2019. ACM.

[43] William Seymour, Martin J. Kraemer, Reuben Binns, and Max Van Kleek. Informing the design of privacy-empowering tools for the connected home. In *Proc. of the CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–14, New York, NY, USA, 2020. Association for Computing Machinery.

[44] Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I. Hong. I'm all eyes and ears: Exploring effective locators for privacy awareness in iot scenarios. In *Proc. of the CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–13, New York, NY, USA, 2020. ACM.

[45] Marc Teyssier, Marion Koelle, Paul Strohmeier, Bruno Fruchard, and Jürgen Steimle. Eyecam: Revealing relations between humans and sensing devices through an anthropo-

morphic webcam. In *Proc. of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. ACM.

[46] Blase Ur, Jaeyeon Jung, and Stuart Schechter. Intruders versus intrusiveness: Teens' and parents' perspectives on home-entryway surveillance. In *Proc. of the International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '14, pages 129–139, New York, NY, USA, 2014. ACM.

[47] Peter Worthy, Ben Matthews, and Stephen Viller. Trust me: Doubts and concerns living with the internet of things. In *Proc. of the ACM Conference on Designing Interactive Systems*, DIS '16, pages 427–434, New York, NY, USA, 2016. ACM.

[48] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proc. of the CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–12, New York, NY, USA, 2019. ACM.

[49] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. Privacy perceptions and designs of bystanders in smart homes. *Proc. of the ACM on Human-Computer Interaction (HCI)*, 3(CSCW), November 2019.

[50] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security & privacy concerns with smart homes. In *Proc. of the Symposium on Usable Privacy and Security*, SOUPS '17, pages 65–80, Berkeley, CA, USA, 2017. USENIX Association.

[51] Eric Zeng and Franziska Roesner. Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study. In *Proc. of the USENIX Security Symposium*, USENIX Security '19, pages 159–176, Berkeley, CA, USA, 2019. USENIX Association.

[52] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home IoT privacy. *Proc. of the ACM on Human-Computer Interaction*, 2(CSCW):200, 2018.

A Interview Script (Study I)

This section provides the interview script used in the first study that investigated the host perspective including slide texts (formatted in italic font).

1. Part: IoT Devices
   (a) Do you currently own an IoT device?
   (b) Which IoT device(s) do you own?
   (c) Why did you purchase the IoT device(s)? For what purpose do you use the IoT device(s)? Are you planning on acquiring more IoT devices? (If yes: Which one(s)?)
2. Part: Interaction with Guests
   (a) How have your guests reacted so far towards your IoT device(s)?
   (b) Did you inform your guests that you own an IoT device(s) or did you make them aware of it/them?
   (c) Have you ever experienced that a guest asks you to turn off your device(s), because the person does not feel comfortable with it/them?
   (d) Have you ever thought about the privacy of your guests in the context of your IoT device(s)?
   (e) Would you give up on your IoT devices' functionalities during the visit of your guest, if the person does not agree with its/their usage and explicitly asks you to turn off the device(s)?
3. Part: Privacy Protection Mechanisms (presented with slides, the text from the slide is given in *italic font*). The order of the first three categories was given by a Latin square. For each mechanism, the participants were asked(1) Would you use the presented mechanism for the privacy protection of your guests?, (2) Please, explain why (not)?, (3) Do you have any suggestions to improve this mechanism?
   (a) Visibility and transparency
      i. verbal device disclosure: *The hosts themselves inform their guests about the existence and use of their IoT devices.*
      ii. dashboard: *The host sets up a dashboard in their home showing all installed IoT devices.*
      iii. physical indicators: *Status indicators help to convey the current status of the device. For example, a sound is played or an LED lights up when the device is in operation.*
      iv. notifications: *Guests receive notifications on their smartphones when IoT devices are detected near them.*
      v. labels: *QR codes are placed on the IoT devices. Guests can scan the QR codes to access information about the IoT device and its data usage. This information is provided by the manufacturer.*
   (b) Privacy Settings and Guest Mode
      i. Settings Access
         – Would you let your guests configure privacy settings on your IoT devices?
         – Would you apply privacy settings configured by your guests to your devices?
         – Who should be responsible for protecting the guests' privacy?
      ii. guest mode without data storage: *The host turns on a guest mode when a guest is visiting. In this case, the data that is captured during the time is not stored.*
      iii. guest mode with device control: *The host switches on a guest mode when a guest is visiting. The guests can enable/disable settings on the IoT device to protect their privacy. Some functions of the IoT device may be disabled.*
   (c) Filtering and Deletion
      i. data filtering: *Data from guests that is captured by a recording device (e.g., audio or video data) are filtered and not considered.*
      ii. data deletion after visit (notification): *Data from the guests, which is collected during the visit, is deleted after a certain time. Subsequently, the guest will be notified about it.*
   (d) Personal Privacy Assistance: *A personal privacy assistant can show nearby IoT devices and information about their data usage. If the host allows it, the guest can change the privacy settings. The app can learn preferred settings and selects them automatically in future situations.*
4. Part: Social Aspects
   (a) Do you think that your guests would be more confident in enforcing their privacy preferences if they had one or more of the presented mechanisms at their disposal?
   (b) Would these alternatives make you feel more comfortable than being asked or approached directly by your guests regarding their privacy concerns and preferences?
5. Part: Demographics
   (a) How old are you?
   (b) What gender do you identify with?
   (c) What is your highest educational degree?
   (d) What is your current profession?
   (e) On a scale of 1 ("not important at all") to 5 ("very important"): How important are data protection and privacy for you?
   (f) Do you have any other comments on the interview?

	Owners				Non-owners			
	Mean	Median	Percentile Q1 (25)	Percentile Q3 (75)	Mean	Median	Percentile Q1 (25)	Percentile Q3 (75)
Requirements								
The owner of the IoT device has little effort for providing privacy protection mechanisms for me, their guest.	3.17	3.00	2.00	3.00	3.20	3.00	2.00	4.00
I, as a guest, have to spend little effort using privacy protection mechanisms.	3.38	4.00	2.00	4.00	3.48	4.00	3.00	5.00
The privacy protection mechanisms are easy to use.	3.50	3.00	3.00	3.00	3.51	4.00	3.00	4.50
I, as a guest, do not have to receive many notifications from the privacy protection mechanism.	3.63	4.00	3.00	4.00	3.60	4.00	3.00	4.00
The owner of the IoT device remains in control over the IoT device and its privacy settings.	3.86	4.00	3.00	4.00	3.98	4.00	3.00	5.00
The functionality of the IoT device is not limited on purpose by the privacy protection mechanism.	3.49	4.00	3.00	4.00	3.55	4.00	3.00	4.50
The functionality of the IoT device is not limited unintendedly by the privacy protection mechanism.	3.34	3.00	3.00	3.00	3.42	3.00	3.00	4.00
I, as a guest, do not have to provide data, such as contact information, to use the privacy protection mechanism.	3.77	4.00	3.00	4.00	3.91	4.00	3.00	5.00
The IoT device does not capture any data from me as a guest without my consent.	3.38	4.00	2.00	4.00	3.60	4.00	2.00	5.00
The privacy protection mechanism does not provide more information about the IoT device owner than required for my privacy protection.	3.67	4.00	3.00	4.00	3.64	4.00	3.00	5.00
I, as a guest, am not allowed to weaken the IoT device owner's privacy settings.	3.90	4.00	3.00	4.00	4.07	4.00	3.00	5.00
The privacy protection mechanism has to be visually aesthetic.	3.00	3.00	2.00	3.00	3.03	3.00	2.00	4.00
The privacy protection mechanism should be clearly visible.	4.03	4.00	3.00	4.00	4.07	4.00	3.00	5.00
The privacy protection mechanism provides assurance about the changes of privacy settings.	3.92	4.00	3.00	4.00	4.00	4.00	3.00	5.00
I, as a guest, know that the IoT device owner approves the privacy protection mechanism.	3.70	4.00	3.00	4.00	3.86	4.00	3.00	5.00
The privacy protection mechanism encourages cooperative configuration by the IoT device owner and me as a guest.	3.18	3.00	3.00	3.00	3.39	3.00	3.00	4.00
The privacy protection mechanism is free of charge.	3.96	4.00	3.00	4.00	4.12	5.00	3.00	5.00
The privacy protection mechanism does not introduce cybersecurity risks for the owner of IoT devices.	3.81	4.00	3.00	4.00	3.64	4.00	3.00	5.00
The privacy protection mechanism does not introduce cybersecurity risks for me as a guest.	3.78	4.00	3.00	4.00	3.76	4.00	3.00	5.00
The privacy protection mechanism can be adjusted matching individual preferences.	3.75	4.00	3.00	4.00	3.93	4.00	3.00	5.00
Changes of the privacy settings by the privacy protection mechanism are limited to the duration of the visit.	3.02	3.00	2.00	3.00	3.13	3.00	2.00	4.00
The privacy protection mechanism is reasonable considering the sensitivity of collected data.	3.72	4.00	3.00	4.00	3.72	4.00	3.00	5.00
I, as a guest, are not forced to use privacy protection mechanisms.	3.43	4.00	3.00	4.00	3.68	4.00	3.00	5.00
The privacy protection mechanism is technically realizable.	3.76	4.00	3.00	4.00	3.85	4.00	3.00	5.00
Impact Factors								
I, as a guest, should adjust to the owner's privacy preferences.	2.95	3.00	2.00	3.00	2.69	3.00	2.00	4.00
I, as a guest, should trust the owner to protect my privacy.	3.63	4.00	3.00	4.00	3.31	3.00	2.50	4.00
I, as a guest, would like to focus on the purpose of the visit and not on privacy protection.	4.07	4.00	3.00	4.00	3.87	4.00	3.00	5.00
The owner of the IoT device should not take it personally when I wish to adjust privacy settings or use privacy protection mechanisms to protect my privacy.	4.01	4.00	3.00	4.00	4.28	4.00	4.00	5.00
Reasons for usage								
I, as a guest, want to be comfortable.	4.68	5.00	4.00	5.00	4.70	5.00	4.00	5.00
The owner should be transparent about IoT devices towards me.	4.03	4.00	3.00	4.00	4.45	5.00	4.00	5.00
I, as a guest, have a right for privacy protection.	4.44	5.00	4.00	5.00	4.72	5.00	5.00	5.00
The IoT device owner values privacy.	3.86	4.00	3.00	4.00	4.00	4.00	3.00	5.00
The IoT device owner is aware of privacy issues.	3.83	4.00	3.00	4.00	3.95	4.00	3.00	5.00
The usage profile of the owner is not impacted or distorted by me.	3.73	4.00	3.00	4.00	3.66	4.00	3.00	4.00

Table 3. Results and Likert-items from the online survey.

B Items and Results (Study II)

This section provides the items from the online survey that were in single-choice, multiple-choice, or open-answer format. The Likert-items including descriptive statistics can be found in Table 3. The participants were asked how important the given statements are for them. The Likert scale items were "I strongly disagree", "I disagree", "I neither agree or disagree", "I agree", and "I strongly disagree".)

Single, multiple-choice, & open-answer items:

1. Has your attention ever been drawn to IoT devices from their owners during a visit? (single answers: yes, no). If yes:
   - How were you informed? (open answer)
   - How did you react? (open answer)
   - Have you ever encountered IoT devices when visiting a friend? (single answer: yes, no)
     - Which IoT devices? (open answer)
     - How did you react to them? (open answer)
2. Would you like to be informed about IoT devices when visiting a friend? (single answer: yes, no)
   - If yes: Why would you like to be informed? (open answer)
   - If yes: How would you like to be informed? (open answer)
   - If no: Why do you not want to be informed? (open answer)
3. Who is responsible for guest privacy when visiting a household with IoT devices? (multiple choice)
   - Guest is responsible to realize their privacy preferences
   - Owner of the IoT device is responsible to learn about and realize the guest's privacy preferences
   - The guest communicates the wish which is realized by the owner
   - Other (please specify)

C Codebook (Study I)

Category	Code	Description	#
Requirements	effortlessness_hosts	Little effort (hosts) during setup or usage	17
	effortlessness_guests	Little effort (guests) during setup or usage	13
	ease_of_use	Mechanism is intuitive or known	7
	unintrusiveness	Guests are not bothered with many notifications	5
	hosts_control	Hosts retain control over IoT devices	17
	functionality_reduction	Functions shall not be restricted	9
	functionality_reduction_acc.	Mechanisms should not "break" functions accidentally	4
	no_guest_data	Guests do not have to provide data	6
	consent_needed	No data collection before the guest has agreed	6
	keep_host_privacy	Mechanisms do not threaten host privacy	7
	no_weakening_privacy_settings	Guest is only allowed to tighten privacy settings	6
	aesthetics	The measure must not be unaesthetic	8
	salience	Mechanisms should be visible	9
	assurance	Guests see or can check settings	5
	social_acceptance	Guests know that hosts agree, usage should be socially accepted	10
	free_of_charge	Mechanisms should not incur extra costs	4
	cybersecurity_host	No cybersecurity risk to hosts	3
	cybersecurity_guest	No cybersecurity risk to guests	1
	customization	Mechanisms should be customizable for guests	2
	reversibility	Effects are limited to guest's visit	5
	appropriateness	Mechanisms should be appropriate to type of data collected	5
	voluntariness	There is no compulsion to use the mechanisms	6
Device Disclosure	influencing_factor	Privacy concerns, collected data, whether guests notice IoT devices, room	14
	reason_refrain	Clarification time-consuming, no complaints, devices do not affect guests	10
	how_to_disclose	Demonstration, loosely (e.g., jokes), during conversation	16
	reaction_guest	How the guest reacted to the IoT device	18
Responsibility	guest	Host unaware of guest's wishes	7
	host	Host's device, their responsibility	11
	both	Guests communicate needs	5
	manufacturer	Manufacturer is responsible	2
Reasons for Usage	guest_comfortable	Guests should feel safe, be satisfied	8
	guest_transparency	Owner wants to be open and transparent	6
	privacy_right	Guests should have control over how their data is handled	8
	profile	Profile of owner not impacted by guest	3
	owner_attitude	Privacy is important to the owner	4
Impact Factors	collected_data	Type of collected data, sensor, or data sensitivity	8
	device_purpose	Purpose if IoT device (convenience or security)	5
	relationship_guest	Closeness of relationship	5
	own_privacy_attitude	Privacy attitude of the host	6
Social Aspects	guests_adapt	Guests should adapt to host's rules	4
	guests_trust	Guests should trust hosts	3
	guest_welcome	Guests should feel comfortable when arriving	4
	owner_not_personal	Hosts do not take criticism of IoT devices personally	3
Improvement	improvement	Suggestion to improve a mechanism	14

Table 4. Codebook used to analyze the interviews.