"I don't know how to protect myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments

Karola Marky
marky@tk.tu-darmstadt.de
Technical University of Darmstadt
Darmstadt, Germany

Alexandra Voit
info@alexandra-voit.de
University of Stuttgart
Stuttgart, Germany

Alina Stöver
stoever@psychologie.tu-darmstadt.de
Technical University of Darmstadt
Darmstadt, Germany

Kai Kunze
kai@kmd.keio.ac.jp
Keio University
Yokohama, Japan

Svenja Schröder
svenja.schroeder@univie.ac.at
University of Vienna
Vienna, Austria

Max Mühlhäuser
max@tk.tu-darmstadt.de
Technical University of Darmstadt
Darmstadt, Germany

ABSTRACT

IoT devices no longer affect single users only because others like visitors or family members - denoted as bystanders - might be in the device's vicinity. Thus, data about bystanders can be collected by IoT devices and bystanders can observe what IoT devices output. To better understand how this affects the privacy of IoT device owners and bystanders and how their privacy can be protected better, we interviewed 42 young adults. Our results include that owners of IoT devices wish to adjust the device output when visitors are present. Visitors wish to be made aware of the data collected about them, to express their privacy needs, and to take measures. Based on our results, we show demand for scalable solutions that address the tension that arises between the increasing discreetness of IoT devices, their increase in numbers and the requirement to preserve the self-determination of owners and bystanders at the same time.

CCS CONCEPTS

• **Security and privacy** → *Privacy protections*; • **Human-centered computing** → **Empirical studies in ubiquitous and mobile computing**.

KEYWORDS

Privacy; Smart Home; Bystander Privacy

ACM Reference Format:
Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. 2020. "I don't know how to protect myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (NordiCHI '20), October 25–29, 2020, Tallinn, Estonia.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3419249.3420164

NordiCHI '20, October 25–29, 2020, Tallinn, Estonia

ACM ISBN 978-1-4503-7579-5/20/10…$15.00
https://doi.org/10.1145/3419249.3420164

1 INTRODUCTION

The market share of IoT devices is steadily increasing [50]. By processing data, the devices can enhance the convenience of everyday life, improve security, or provide better control over energy consumption [27, 36]. Therefore, the devices collect data via sensors and output it. Both - collection and output - concern *anyone* that is present in the smart environment. Therefore, it is crucial to consider different people in smart environments: primary users and indirect users. Primary users interact with IoT devices to achieve specific goals, such as controlling the lighting. The group of indirect users includes residents and visitors of the smart environment. However, only specific users, i.e. the owners of the IoT devices can configure them. In this paper, we denote them as *owners.* Visitors of the smart environments, e.g., repair staff or friends, can observe the output of IoT devices without interacting with them. In this paper, we denote these indirect users as *bystanders.* The constellation of users and bystanders is also crucial in the scope of privacy.

The privacy of the bystanders might be violated by IoT devices without the bystander noticing it [46]. A smart speaker might record a conversation of guests, or a camera in a fridge might film guests who open it [30, 31]. On the other hand, the presence of bystanders in a smart environment might also pose a privacy threat to IoT device owners since the bystanders can witness the output of IoT devices. For instance, a smart speaker might remind an owner to check their emails for medical test results and the bystanders hear that. Based on this constellation of bystanders and owners, it is important to consider *both* user groups when designing privacy-respecting IoT devices and environments. Previous studies glimpsed into the individual user types and for instance recommended a visitor mode [60, 61], means for bystanders to exert control [59], or provision of different levels of agency [18]. In this paper, we present a comprehensive investigation of the owner-bystander constellation from both perspectives. In particular, we aim to shed light on the following research questions:

RQ1: What are considerations of IoT device owners when installing and configuring devices in their homes?

- **RQ2:** What kind of information are IoT device owners comfortable sharing with bystanders?
- **RQ3:** What are the perceptions of bystanders regarding privacy in a smart environment?
- **RQ4:** What are the coping strategies of bystanders to protect their privacy in smart environments?

To answer our research questions, we conducted semi-structured interviews with 42 participants. Among other aspects, we found that only a few owners consider privacy when installing devices in their homes. However, they wish for detailed options to control the information that is output in the presence of bystanders. Even urgent information, such as an emergency in the family, should be protected. Concerning the bystanders, we confirm and extend results from other domains, such as life logging [10, 14], showing that bystanders wish to exert control over their data collection. We furthermore demonstrate that bystanders lack actionable measures to exert control over the data collection. Based on our results, we conclude that solutions provided by existing IoT devices are not sufficient and do not scale. There is a demand for new solutions that reduce the burden on owners and bystanders and support them effectively in making and realizing their privacy decisions. However, current developments make IoT devices more discreet and their number will increase in the future. This makes it difficult for owners and bystanders to make adjustments to protect their privacy for each individual IoT device. Our study indicates that there is a tension between the self-determination of owners and bystanders and the ongoing advancements of IoT devices. Finally, we name challenges for the design of future smart environments that consider privacy aspects based on the owner-bystander constellation.

2 BACKGROUND AND RELATED WORK

In this section, we detail the *privacy* definition that we based our investigation on. Then, we present related works on *privacy concerns in smart homes* and *bystander privacy*. Adding to this body of research, our paper focuses on the privacy concerns that might arise from the presence of bystanders in smart environments. We investigate the views of owners and bystanders in-depth.

In this paper, we consider *privacy* as the possibility for users to control the circumstances and conditions under which their personal information is collected and processed by a third party [12]. Thus, each user individually decides about their private data and privacy is not an absolute term.

General perceptions and attitudes towards ubiquitous technologies have been investigated in the literature. This stresses that privacy is an important topic in the scope of HCI. Tracking by devices that are used on a daily basis, such as credit cards, constitutes a major concern [42]. Also, IoT devices have been investigated [44]. The privacy concerns and perceptions of (prospective) users of different technologies have been investigated in a variety of domains (cf. [33, 34, 62]).

2.1 Smart Home Privacy Concerns

IoT devices require access to data about their users and the users' environments which can lead to privacy concerns [1, 51, 58]. The perceptions and concerns of (prospective) owners of IoT devices have repeatedly been studied in the literature [2, 4, 7, 9, 11, 15, 57, 60, 62]. Naeini *et al.* found that the privacy perceptions are dependent on the context and users differentiate between different environments and data types [15]. In particular, they perceive the collection of their data in public environments as less critical than in private ones. Furthermore, they consider data about their environment (e.g., room temperatures) as less critical than data about themselves. Finally, Naeini *et al.* report that perceived benefits constitute a major factor when consenting to data sharing. The role of the perceived benefits has been confirmed in an interview study by Zheng *et al.* in which they focused on the experiences of eleven smart home owners [63]. Owners are also willing to share privacy-sensitive data with service providers if the data was anonymized [29].

When asked for specific concerns, people mention concerns about the physical security and general privacy of the home [60, 64, 65]. On the other hand, a study by Zeng *et al.* has shown that many smart home owners were generally not concerned about potential threats [60]. Owners only expressed little privacy concerns about the nature of the data but strong concerns on how the providers of smart home devices handle the data [49]. Lay owners expressed difficulties in naming specific consequences that could arise from sharing smart home data [21]. But smart home owners should be aware of potential consequences to be motivated to configure the system so that it matches their privacy needs [21, 28].

Different studies revealed that smart home owners wish to be aware of data that is collected and transferred to providers [15, 24, 40]. An interview study with 23 smart home owners examined their perceptions of devices, data practices, and risks [51]. The results confirm that owners are uncertain about the data practices of the companies and wish for more transparency and control. Being asked to create a design that respects smart home privacy, participants in a study created designs that aimed to increase the transparency of data collection and allow the owners to control the data collection [58]. Users wished to be informed about the privacy aspects of the devices before purchase [16].

Besides smart homes in general, also the perceptions and concerns regarding specific devices have been investigated in related work. The awareness of the data collected by smart TVs has been investigated by Ghiglieri *et al.* [22]. The authors found that users of smart TVs are generally not aware of the data collected by their devices. When informed about it users tended to disconnect their smart TV from the network. Even though the majority of online reviews about smart speakers do not mention privacy concerns, users expressed to have mixed feelings [17]. Some users of smart speakers do not use their full functionality due to privacy concerns and do not want those smart devices to learn sensitive information about them, such as health symptoms [1].

A diary and interview study investigated the perceptions of seventeen users of smart speakers [31]. The study shows that privacy tensions may arise between primary, secondary, and incidental users. Although 73% of the study participants lived together with others, such as roommates or family members, none of the participants considered privacy while placing the smart speaker in their home.

2.2 Bystander Privacy

In this paper, we consider privacy perceptions from owners and bystanders. Hereby, we consider *bystanders* as passive observers who do not engage in any activities that might aim to break the privacy of the smart home device owner. But the bystander might learn privacy-sensitive information via notification output from the devices. On the other hand, the privacy of the bystander might be violated by smart home devices that collect data in the bystander's environment [46]. In the smart home context, bystanders can be either residents or visitors.

Bystander privacy has been investigated in different emerging technologies, like lifelogging with wearable glasses or cameras [23, 25, 47], augmented reality [3, 10, 56], multi-user augmented reality [32], and mixed reality [13, 41, 45]. The privacy perceptions of bystanders in the surroundings of visually impaired users that use assertive technologies have been investigated [3]. Bystanders would share information for assertive uses and would share even more information if they can exert control over it. The users of lifelogging-technologies generally aim to preserve the privacy of bystanders when sharing their data by establishing rules [47]. The concerns of bystanders regarding the presence of augmented reality wearable devices are dependent on the context as two studies show [10, 14]. The participants differentiated between public and private places. They articulated that at recording in places, like bathrooms, bedrooms or in other homes, it would be unacceptable and wanted to be asked for permission before being recorded.

The existing works in the scope of privacy concerns in smart homes primarily focus on smart home users. Some works uncovered concerns about the individual privacy of other smart home inhabitants [39, 52]. For instance, minors living in the household might express discomfort that the parents can monitor them. Thus, parents have to balance respecting their children's privacy with monitoring their children's activities [38, 48, 52]. Several studies investigated multi-user scenarios in smart homes with multiple residents [18, 19, 58, 60, 61]. Privacy aspects can be negotiated among different inhabitants [19]. On the other hand, the complex social relationships and power dynamics within a home can also complicate privacy aspects [58]. Yao *et al.* asked their participants to design privacy-respecting smart home devices [58]. Even though the majority of designs only considered smart home residents, some designs also aimed to protect the privacy of visitors. Although not specifically investigating visitors, two studies show that smart home residents wish to have a visitor mode of devices [60, 61].

Another stream of related work indicates that owners of smart home devices can consider the presence of bystanders as a privacy threat. Participants in a study that investigated the display of notifications on smart windows wished an option to switch off the notifications if visitors are around [5]. Yao *et al.* studied three specific scenarios in which the privacy of bystanders in smart homes can be relevant [59]. They conducted a co-design study to identify factors that impact and mitigate the concerns of bystanders within these scenarios. Their most prominent finding was the wish of bystanders to exert control over data collection.

3 METHOD

To investigate privacy perceptions that arise from the presence of bystanders in smart environments, we conducted a series of user studies. We commenced with a *pre-study* to collect a set of possible bystanders. Then, we proceeded by *semi-structured interviews* with a total of 42 participants.

3.1 Pre-Study

To collect a set of bystanders that can be present at someone's home, we conducted an online survey. After declaring their consent and providing demographics, the participants received lists of possible bystanders. We asked the participants whether these people visited their homes and to supplement the list of other people that are present in their homes or visiting them. We recruited 131 participants via mailing-lists and did not reimburse them for taking part in the survey. 40% of the participants identified as male, 59% identified as female, 0.5% identified as other, and 0.5% did prefer not to provide this information. The average age of the participants was 28.8 years ($SD = 9$, $Min = 18$, $Max = 67$). The resulting list of bystanders contains eleven types of relatives (e.g., parents), ten types of known persons (e.g., friends), and four types of strangers (e.g., craftsmen-/women).

3.2 Semi-Structured Interviews

To investigate the privacy perceptions of bystanders and owners, we conducted semi-structured interviews with 42 participants in two groups. The first interview group investigated the *bystander view* of people who are either residing in a smart environment or visit it. The second interview group investigated the *owner view* of those who are installing and configuring IoT devices. We opted for semi-structured interviews because they offer a degree of standardization while also leaving room to investigate the answers of the participants in more depth [43]. Before determining our final interview questions, we conducted two exploratory interviews for each view. We adapted our questions and explanations to improve their clarity. The results of the pilot interviews are not included in our results.

3.2.1 Interview Procedure. The procedure of the interviews was as follows (see also Fig. 1).

1) Welcome. Before the interview, each participant received a consent form describing the study's data protection policy and its procedure. Neither the consent form nor the study invitation mentioned that the interview would be about privacy to avoid priming of the participants. After signing the consent form, each participant provided demographics.

2) Understanding. We commenced the interview by letting the participants explain their understanding of a smart home. Then, we introduced the definition of a smart home that we use within the research project to establish a common understanding. We answered questions regarding this definition and made some examples of smart homes together with the participants. Next, we asked the participants about their experiences with the usage of smart home devices.

3) Scenario Introduction. In this part of the interview, we introduced the participants into the scenario matching their group. We used the scenario to nudge the participants to think as owners/bystanders. We made sure that the participants understood the

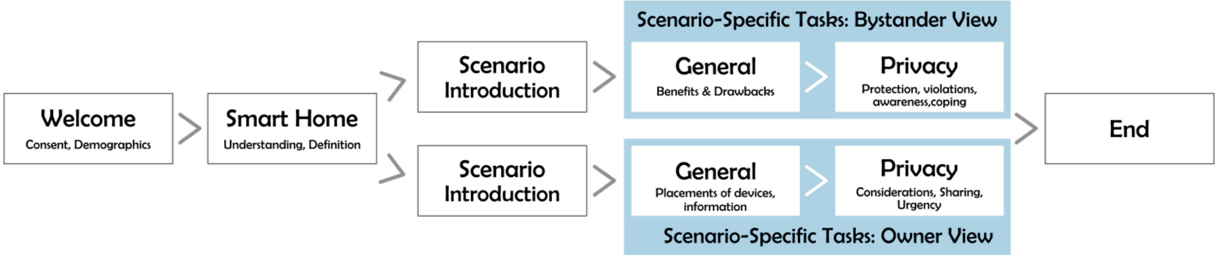
Welcome
Consent, Demographics
Smart Home
Understanding, Definition
Scenario Introduction
Scenario Introduction
Scenario-Specific Tasks: Bystander View
General
Benefits & Drawbacks
Privacy
Protection, violations, awareness,coping
General
Placements of devices, information
Privacy
Considerations, Sharing, Urgency
Scenario-Specific Tasks: Owner View
End

Figure 1: Schematic depiction of our study procedure.

assigned scenario and answered questions about it. Dependent on the interview group, the participants received different tasks and questions about the scenario.

4a) Scenario-Specific Tasks: Bystander View. In the bystander view, we commenced by asking the participants for their perceived benefits of smart homes. Within this question we asked the participants to consider 1) benefits for the owner of the smart home, 2) benefits for other people that reside in the smart home, and 3) benefits for visitors. We kept this differentiation throughout the remainder of the interview. The next question was about the perceived disadvantages. We asked this question to investigate whether the participants mention privacy before introducing it.

Next, we introduced privacy and the definition that detailed above. After establishing a common understanding of privacy, we asked whether the participants consider the privacy of the owner, other residents, and visitors to be protected. Then, we asked them which party or person can be responsible for privacy violations in their understanding.

Then, we investigated the participants' perception of specific IoT devices that are already available on the market. We provided a list of the devices, their main functionalities, and the data that they can capture. Although all devices are available on the market, we did not mention manufacturers to avoid confounding with the participant's opinion of that manufacturer. In particular, we considered the following devices: smart assistants, smart screens (e.g., a TV), smart household devices (e.g., a fridge, vacuum or thermostats), and smart surveillance systems. We asked if the participants consider it problematic to visit a household with such devices and whether they consider their privacy to be protected. Then, we asked them whether they consider it necessary to protect their privacy and how they would like to protect it. Hereby, we asked the participants for specific measures.

4b) Scenario-Specific Tasks: Owner View. In the owner view, we wanted to investigate how (prospective) owners of IoT devices place them into their homes. We commenced by introducing five types of IoT devices since those device types are available on the market and provide different output modalities: 1) smart assistants, 2) standalone smart screens (e.g., a TV), 3) integrated smart screens (e.g., in a mirror), 4) smart light bulbs, and 5) control screens. During the introduction, we also explain the devices' output modalities, i.e. graphical, textual, sound, and light patterns. Once the participants were familiar with the devices, we asked them where they would place them in their homes. Therefore, we used a bulletin board and cue cards. We had multiple cue cards with the devices and the participants were asked to pin them next to the room where they would place it. While device placement, we encouraged the participants to think-aloud. The participants could also add additional rooms.

In the next part, we asked the participants which information should be available on the devices that they just had placed. Therefore, we provided the participants with a list of possible notification information categories that we obtained from the literature [54]. While assigning information to the devices, the participant was again encouraged to think-aloud. Now, we provided the list of bystanders from the pre-study and asked which information the participants wish to share with bystanders at their homes. Finally, we introduced the concept of urgent information which is information that the owners should receive immediately, such as an emergency. Considering urgency, we asked the participants if and how they would change the assignments on the bulletin board.

5) End. After the interview, we explained that the interview was focused on privacy and we gave the participants the opportunity to ask questions or to give additional feedback.

3.2.2 Participants. We recruited 42 participants, 21 for each view, via mailing-lists, posters, flyers, and by snowball sampling. They were on average 26.4 years old ($SD = 5$, $Min = 21$, $Max = 55$). 34% of participants identified as female and none as "other". The invitation did not contain any information that the study investigates privacy, instead, it only mentioned an investigation of perceptions of (potential) IoT device users. Thus, the study was restricted to participants that either own IoT devices or are interested in owning them in the future. 54% of participants reported having never used IoT devices that are networked among each other, 2% used them in the past, 25% reported to use single IoT devices and 19% reported active usage. 38% of the participants reported having visited a foreign smart environment before, 15% did not know whether they have visited a smart environment before, and the remaining 53% visited households with single IoT devices (e.g., one smart speaker). We did not reimburse the participants for participating in our study.

3.3 Data Coding

We analyzed the interviews using the grounded theory approach [37]. Before the analysis, the interview recordings were transcribed. Privacy-sensitive data, e.g. names of relatives, was replaced by neutral placeholders. After the transcribing, the audio files were deleted.

Two researchers individually coded two representative interviews for each view using thematic analysis with open coding [6]. In a review meeting, a coding tree with 320 codes for both views was established. For each view, one researcher coded all interviews using the coding-tree. Through axial coding, the codes were related to one another which resulted in the creation of three main categories in the bystander view, and four main categories in the owner view.

3.4 Ethical Considerations

The ethics committee at our institution provides a set of guidelines for user studies. Our studies follow these guidelines. In doing so, we limit the collection of personal data to a minimal amount in order to preserve the privacy of our participants. Each participant received a randomly assigned identifier that we used throughout the studies and analysis. Before taking part in the study, each participant received a consent form that also contained the study's data protection policy. Participants were asked to read and sign the consent form which was then stored separately from all other captured data. Our study, furthermore, complied with national privacy regulations and the European General Data Protection Regulation (GDPR). Our institution is located in a country with no requirement for following a formal IRB process for the kind of user study that we conducted.

4 RESULTS - BYSTANDER VIEW

In this section, we describe the results from the bystander view with a focus on the findings related to bystander privacy. We provide participant comments when meaningful.

4.1 Privacy Aspects as Perceived Disadvantage

The participants in the bystander view named several disadvantages of smart homes. Those include the additional complexity of the devices that might increase their cost and assembly time ($N = 10$), but also security-related aspects, such as bugs in the software ($N = 11$) or hackers that might gain access to the devices ($N = 14$). We asked this question before introducing privacy into the interview to find out whether the participants consider privacy by themselves.

The participants almost equally often mentioned that the privacy of other residents that do not control the smart home devices ($N = 16$) and of visitors ($N = 13$) might be violated. On the other hand, only 38% of the participants considered smart home devices to be beneficial for visitors. The only reported benefit was an increased convenience by automation. Sample comments that mention the privacy of bystanders are: P6 said *"Guests know nothing about the captured data, they don't know where it's stored, when it's deleted and not even why the data is collected."* And P13 stated: *"As a visitor, I don't know what's happening [...] is my voice recorded the entire time? Someone could access that and the admin has access anyway."*

4.2 Privacy Perceptions

After introducing the privacy definition to ensure a common understanding, we focused the interview on privacy. We asked the participants whether they consider privacy in a smart home to be protected. Again, we used the differentiation of the owner, other residents, and visitors.

4.2.1 Trust Aspects. Participants expressed that trust towards the owner of the device or the provider of it is required. If the owner was a friend or a person that they know well, some consider their privacy as a visitor to be protected ($N = 7$), for instance, P4 said: *"That would then depend on whom I go to, whether I trust them or not and how well we know each other."* Four participants also considered that the provider of the device has to be trusted, for instance participant P10 said: *"So that they [visitors] just have to trust that the administrator and the company, which offers and operates the network, do their job properly and make sure that the privacy which they have as visitors, is protected."* These trust aspects were exclusively mentioned in relation to the visitors of smart homes and not in connection with residents.

4.2.2 Lack of Awareness. Since the smart home devices commonly are everyday devices, seven participants expressed difficulty to judge whether a device can collect data. Without further information or knowledge of the device, visitors cannot gain adequate awareness without the cooperation of the device owner: *"It's even worse than for residents, they [the visitors] may not even know anything about it."* (P1) and *"I wasn't aware of it that the device could theoretically violate my privacy."* (P2)

4.2.3 Lack of Concern. Some participants did not feel concerned about the devices because those are not personalized for them as visitors. This indicates that people might think that registration on the device is necessary for the device to capture data about this specific person: *"Depends on how intelligent the system is. So I'm assuming that the smart home is stupid for visitors and others it's not configured for. Then, I think that privacy is a bit different. Because the system doesn't know the people. They are anonymous for it."* (P6) Another lack of concern results from a rather rare presence of visitors in smart homes. Meaning that rare presence results in amounts of data that are too small for a privacy violation: *"I will also be monitored, my data will be stored. But not as much as the owner or the people who live there permanently."* (P11) and *"I think the visitors' privacy is protected because they only interact with the smart home once in a while."* (P2)

4.2.4 Parties that Violate Privacy. Six participants considered their privacy to be violated by another user of the devices because they could access their data. Two participants stated that the device owner might unintentionally disclose their data. Seven considered the device provider to be able to violate privacy by accessing the data. Furthermore, seventeen participants considered external attackers, such as hackers, to be a source of privacy violation. In this scope, the participants did not differentiate between residents and visitors and considered them equally. Sample comments from the participants are: *"The owner could read the data from the roommates, and then determine their habits."* (P12). Participant P8 stated *"The owner could, perhaps somehow pass data to third parties, maybe without knowing."*, and P13 said *"Of course, it may be that some hackers or so get access to some data."*

4.3 Coping Strategies of Visitors

When presenting a list of the smart home devices that are already available on the market, we asked the participants about their experience with such devices and whether they as visitors would like to protect their privacy from them. The participants communicated various coping strategies that they either actively use, or that they wish to use. Some reported that they do not want to use any coping strategy.

4.3.1 No Coping Strategy. Five participants would not take any measures for various reasons, those include a perceived comfort that is only received by sacrificing privacy ($N = 2$): *"Someone who runs it won't probably put the worries under the comfort because the comfort is probably more important to [them], otherwise, [they] wouldn't run it."* (P4) Two participants stated the above-mentioned lack of concern and resignation as a reason: *"A mixture of disinterest and resignation? In the end, my things like my voice are all over the place anyway, and my statements and I'm spreading everything I have to say everywhere anyway."* (P18) and *"I'm a very gullible person [...] I've never had any bad experiences and so I'm probably a bit too generous sometimes when I share such data, order things over the internet or whatever. So sometimes I'm too open and probable, but as I said I've never had any bad experiences."* (P8)

4.3.2 Status Communication. Similar to other domains in which data is collected, three participants wish to gain knowledge about the device's status to judge whether they need to take measures: *"It is important to me that especially delicate topics are not recorded by a speech recognition system, and that I have the possibility to check whether speech recognition is really off."* (P10) Status communication is considered as a way to assess the current state of data collection in the surroundings. Some participants said that the device owner could also inform them about the device or even expect the owner to do this without prompting: *"I'd like to know. Let's put it this way. I'd like to know, then it's something else, then I could live with it, but I'd like to know."* (P1)

4.3.3 Switching Off. Switching the device off or asking the owner to do so was mentioned by five participants. However, two of them only considered it in a hypothetical way meaning that they consider it to be a good measure but would not apply it in reality. Participant P11 said *"[...] asking the host to turn off the data storage. Because that's going to be a relatively small amount of collected data coming from me anyway, but I can't imagine now that's for a short visit I'd do something like that, but, yeah, that'd be more relevant to the people who live there than to short visitors."* and P14 stated *"I mean the only measure is switching it off. Or not going there at all."*

4.3.4 Deletion of Data. Three participants wished a possibility to delete data that was collected about them. Depending on what they did in the foreign smart environment, they want to decide if the data is kept or not when leaving. E.g., participant P10 said *"That you have the possibility to view this and possibly delete the recordings yourself so that you can go to the person who administers it and tell him 'you wouldn't like it if recordings were made by me tonight, please make sure that they are deleted'"*

4.3.5 Jamming of Data Collection. Three participants would like to jam the data collection: *"[...] you have a smartphone or something like that with you, it sends out an interference signal or something, so that the speech or something can no longer be recorded."* (P5) But on the other hand, they considered this as an overreaction: *"If you were really hard on it, you could take a jamming transmitter with you, for example, but it's also a bit too much, I think."* (P9)

4.3.6 Adaption of Behavior. Four participants would even change their behavior in the presence of IoT devices. They either would refrain from visiting: *"If I were a visitor more often, I think I would be uncomfortable, but if I am only there a few times, it wouldn't be a bigger problem for me. So I wouldn't try to protect my privacy but I wouldn't go there so often."* (P15) Or they would adapt the content of their conversation: *"So I wouldn't necessarily mention private details in the presence of such a device, which nobody else should hear."* (P9)

4.3.7 Lack of Applicable Coping Strategies. Besides the specific strategies mentioned above, participants expressed helplessness in finding an applicable coping strategy. Four participants thought that the ubiquity of IoT devices in the future will make it impossible for them to take measures in the future. Besides not visiting the smart environment they feel as if there was no possibility to escape it: *"I don't think you can really fight it, yet."* (P6) and *"I don't know how I could protect myself If there was something to do I would do it, but I simply don't know how."* (P18)

5 RESULTS - OWNER VIEW

We describe the results from the owner view. Hereby, we focus on the findings that are related to privacy.

5.1 Privacy Considerations during Device Placement

When we asked the participants to place IoT devices in their homes, the majority ($N = 15$) did not consider privacy aspects. Instead, participants primarily focused on replacing existing devices with their smart counterparts, on the functionality of the devices, and how/where they could use it in their daily lives. Five participants considered privacy and wanted private information in restricted areas only: *"I think everyone in the living room can usually access everything, and private information such as messages or emails should be displayed in the private bedroom."* (P31) and P24 stated *"In the best case, I would put it [integrated smart screen] in places where other people can't get to, so bathroom and bedroom. We have an extra toilet for guests."*

In addition, two participants avoided placing smart speakers in areas where chats with private content could be recorded by these devices. P33 explained *"[...] where I know that I'm gonna have personal conversations, there's no microphone coming in. And especially my bedroom, that's my private room in my flat, there's no microphone connected to the internet."* And P34 said *"Consider the smart assistant, definitely not in the bedroom, especially if now potentially the data might be shared with the police. That would simply be too big a breach of privacy. "*

5.2 Privacy Considerations during Information Assignment

The majority of the participants ($N = 14$) did not consider privacy while assigning information output to the devices. Participants rather focused on which kinds of information they would like to access in their daily lives: *"I haven't given much thought to who actually sees it but it would make sense. Because when you have* *something hanging in the hallway and someone whom you don't know well passes, you don't necessarily want him to know when and where you are. Then that would have been worth a thought. But that's just my personal preference that I'd like to see when I'm alone."* (P22)

One participant, however, was aware of privacy issues but felt helpless in addressing them: *"It's important to me that not everyone can see everything [...] Considering the control screen, everything is on it. And when I get home, I'm first in the hallway, and when I realize I've forgotten something or there's something important, I have the view right in the hallway. But everyone else also has the view. Then there's the problem."* (P41)

Four of the participants who already considered privacy during device placement also preferred showing private information only in specific areas in their homes such as their bedrooms where others typically do not have access: *"I've been mentioning the limitations all along while assigning. The mirror [integrated smart screen], for example, is in my bathroom, bedroom, and hallway. Messenger things and certain calendar things would be bad for the hallway."* (P27) and *"If I had one of those screens in my bedroom, I'd show something different than if it was hanging in the hallway. So if it's in the public area, I wouldn't show my fitness data in any case. Maybe I'd leave it on my mobile phone, but if it's on the bedside table, I could imagine it."* (P30)

Two participants assumed or wished the smart home to provide options to adapt the displayed information depending on present bystanders. P24 stated *"Generally I would say that there is a mode where you can set if friends are there that the calendar will not be displayed, or with face recognition that only things that affect the person will be displayed."* Participant P36 explained: *"Calendars also everywhere, but it would be nice if you could set the events with different levels [of access], so for everyone, for fewer people."*

5.3 Information Sharing with Specific Bystanders

In this part of the interview, we consider the sharing of information with specific bystanders.

5.3.1 No Restriction on Public Information. In total, 17 participants stated that information that is not privacy-sensitive to them can be shared with everyone. This concerns notifications from the category tool which contains information about publicly available data, such as weather conditions or news:
"I would add tool for everyone. That [does] not contain anything bad [such as] weather or anything else." (P23)

5.3.2 Restriction on Household-Related Information. Information that concerns the household is only shared with people that are affected by it, but 16 participants do not mind sharing information that is obvious to bystanders such as the status of household devices: *"Whether the dishwasher has finished or not is irrelevant, therefore information regarding the dishwasher or that the plants must be watered, I would show everyone, but whether food is expired I wouldn't share, except for my partner."* (P24) *"Household. That concerns all, who live there and who comes to visit is also ok [to share information with]."* (P30)

In addition, two participants stated that it would be beneficial to share household data with other close persons, such as friends or family members, to enable them to support them in their homes: *"So friends and acquaintances I would trust, too, if they see that the plants have to be watered, they can water them, but with strangers who don't need them, they don't do that."* (P31) and another statement *"If you have some [children] they can help in the household if the dishwasher is done they stow away the dishes."* (P38)

5.3.3 No Sharing of Messages. In contrast to the information sharing explained above, the majority of participants ($N = 16$) stated that personal messages, such as instant messages and e-mails, should be kept private and not be available for any other person. Hereby, the participants stated that the content of the message is unknown and hence not predictable. Furthermore, they stated that messages are considered as private data. P23 said *"It could be that a mail comes that concerns a secret gift for my partner and then he would see it."* P22 focused on the decision possibility: *"I don't know which message is coming in from whom, I would rather not want anyone to see it, and if I want to show it to someone, I want to decide for myself, so I wouldn't assign it to anyone."* And P25 mentioned privacy aspects: *"My emails do not necessarily have to be read by my partner, even if I have nothing to hide there, I find this simply does not concern others."* Twelve participants wanted a reduced amount of information in the notification. Instead, the message content should be only metadata, such as the sender or even just that a message is there: *"If you could just see "a new message from [name]", I wouldn't care. But I've already concluded that you see the messages and that's privacy for me."* (P41)

5.3.4 Sharing for Personal Benefits. Seventeen participants would share their data to gain a personal benefit. Among those the sharing with professionals was prominent: *"Well, [sharing with the] domestic help, wouldn't be bad if [they] had access to household to know what to do."* (P32) Further, 16 of the 17 participants wanted to share health-related information with medical personal that visits their house: *"I think, my doctor may see my health data because with [them] the whole health data runs together anyway. Therefore my doctor would be trusted with my Health/Fitness data."* (P33) In contrast to that, another two participants mentioned sharing the data with professionals could become problematic even if there is a personal benefit: *"It is potentially appropriate [to share with] care professionals, but the health insurance companies are considering collecting the information voluntarily to adapt the fees, which I regard as very critical, which is why I would not give [them] access from the outset. This also applies to health professionals and doctors."* (P34)

5.4 Privacy versus Urgency

All participants wanted to receive sensitive but urgent or critical information in the presence of others. The majority of the participants ($N = 15$) suggested that the smart home should convey abstract notifications without displaying the specific content. P30 explained *"So if there really isn't any other way, then it wouldn't be a problem, just because the alternatives are missing. I could imagine that people would just tell me that there's something [a notification] there, and I'd get the details from a different source, so the other people wouldn't get it."* The remaining participants ($N = 6$) stated that they would even like the content to be displayed in the presence of bystanders: *"I have to react to it, I don't care if someone else notices it, there are* *more important things in the situation. If there is critical information, I would say I could be told that there is important information, but if I let someone into my house I trust them that critical information would be fine."* (P34)

6 DISCUSSION

Since IoT devices are designed to affect the environments of their owners, they also affect other people. The results of our study reinforce that the bystander-owner constellation needs to be considered when designing smart environments and devices. Existing IoT devices do not consider the presence of bystanders, hence both owners and bystanders struggle to adjust the IoT devices matching their privacy needs. In the remainder of this section, we first discuss our interview results and derive challenges for designing future smart environments. We then detail *opportunities for future investigations*, and reflect on *limitations* of our work.

6.1 Awareness and Mode Transparency

Awareness of data collection and processing played an important role in both investigated views. It refers to the degree to which a person is aware of the organizational information privacy practice [35]. To gain awareness bystanders need to know about the presence of IoT devices. Our study shows that visitors of smart homes might struggle in judging whether a device is indeed a smart device because familiarity with the device is a prerequisite. Our study also shows that bystanders wish for mode transparency, which extends results from life-logging studies [10, 14]. In particular, they wish for means to assess the current state of the device, such that they can easily judge whether the device currently captures their data. Since the number of devices is likely to increase in the future, IoT device owners should not only be responsible for that, the device itself should communicate its status in an understandable way, such as status indicators [8, 26]. Nowadays in 2020, the majority of IoT devices are easy to spot but the ongoing development of IoT devices will result in devices that are more discreet. Therefore, bystanders might struggle even further in gaining awareness.

While owners of IoT devices can be aware of the data that is collected by them, they might be unaware that the output of the device might violate their privacy if bystanders are present. The majority of participants in our study did not intuitively consider privacy while assigning information to IoT devices. This extends previous results about smart speakers [31]. But the share of participants who indeed considered privacy shows that people can be concerned about the device output. This has also already been indicated by studies of specific IoT devices, e.g., smart windows [5].

After making the participants aware of privacy, the majority of them realized this aspect. On the one hand, this might be related to the so-called privacy paradox meaning that participants in user studies express to value their privacy but in reality demonstrate a different behavior [20]. On the other hand, the distribution of smart homes in 2020 is still rather low and (prospective) owners might not have been confronted with such privacy aspects yet. Even if the owners are not aware of the potential privacy violations by bystanders during device installation, they can proactively react when bystanders are present. However, a violation cannot be undone by this reaction.

6.2 Fewer Benefits for Visitors

When interacting with technology, users consider a ratio of the perceived benefits from that technology and the amount of individual-specific data possessed by third parties [35]. This ratio has already been investigated for IoT device owners and the added convenience is the main reason for sacrificing privacy [15, 63]. Our participants expressed that visitors are less likely to benefit from the functionality of IoT devices. Visitors that are unfamiliar with the specific device might even be unable to use it. Still, their data is collected and processed by it which calls benefits for visitors into question. Our participants also demonstrated difficulties in naming benefits for bystanders besides an enhanced convenience. But this convenience rather affects smart home residents because bystanders only rarely interact with household devices. Therefore, the participants were concerned about their data being collected when visiting a smart home. This extends previous results from other domains [10, 14]. Even if smart home visitors are aware of the data collection, they do not know how the data is processed or stored. The receiver of the data is not apparent to them and they do not know for how long the data will be stored.

6.3 Exerting Control

In both views, the participants expressed the wish to exert control. In the bystander view, smart home visitors would use different coping strategies to control how data about them is captured. Some participants even considered not visiting the smart home at all or adapting their behavior. Exerting control is not supported by all current IoT devices, except for the obvious: switching them off. Based on that, participants in our study expressed perceived helplessness and a lack of coping strategies to protect their privacy. This indicates that future IoT devices should provide means for bystanders to adjust them. This, however, constitutes a fundamental challenge, since the views of owners and bystanders might be conflicting, as it has been shown by studies of multi-user scenarios [47]. Participants in both views wished to have a visitor mode which confirms the results of previous studies [19].

Although it seems to be obvious that the IoT device owners have control regarding the sharing of their data, the awareness aspects above might result in an initial privacy violation that the owner has to react on. In other domains, such as notifications on multiple devices, it has been shown that users tend to circumvent dealing with such issues by either not acting at all, or by uninstalling the corresponding app [53]. An investigation of privacy settings for notifications on public displays revealed that users opted for generic settings that work for a variety of content [55]. While they welcomed the settings, they did not want to spend time configuring it. This indicates that privacy by design is of importance. Participants in our study expressed helplessness in configuring current devices according to their needs. Some participants even expected IoT devices to react to the presence of bystanders.

6.4 Misconceptions

Participants in the bystander view showed misconceptions regarding the data collection in a smart home. Owners and bystanders thought that registration on the device is necessary that such data of a person is collected. While it is true that the device cannot immediately connect the data to a specific person without such a registration, the data set of the person might be growing over time, making identification more likely [11]. Furthermore, data could be matched to a person based on information that is available from other sources, such as social networks. This also encompasses data from visitors that rarely visit the smart home or visit it just once. Participants expressed that the data of such rare visitors are protected which in general is untrue. This misconception shows that the mental models of our participants do not correspond to reality. This demands methods to properly inform owners as well as bystanders about the consequences and power of data collection as already suggested by other works [21, 28].

6.5 Challenges in Designing Future Smart Home Environments

Summing up, the presence of bystanders in IoT environments results in the following four challenges that need to be addressed by the designers of future smart environments:

6.5.1 Awareness Challenge. Owners, as well as bystanders, have to be supported by the IoT devices to gain awareness about the status of the respective IoT device. The proliferation of IoT devices, their growth, as well as their increasing discreetness demands solutions that go beyond status communication.

6.5.2 Decision Challenge. Bystanders, especially visitors, cannot gain adequate information on the smart home ecosystem, i.e., how their data is processed and stored. They might even have misconceptions that hinder them in making a decision that matches their privacy needs. Informing bystanders and adjusting their mental models to support them making their decision constitutes a fundamental challenge since the growth of smart environments would demand bystanders to make many decisions.

6.5.3 Mode Challenge. Owners and bystanders wish for a device mode that considers the presence of bystanders. Based on the heterogeneity of IoT devices, the introduction of such a mode is not trivial from the bystander perspective. While owners could configure such a mode to match their privacy needs, there should also be a way for bystanders to reflect that. Analogously to the awareness challenge, increasing discreetness and number of IoT devices demand solutions that go beyond a simple visitor mode. Means for bystanders to express their needs are required in a scalable manner.

6.5.4 Support Challenge. Ordinary owners and also bystanders cannot be considered to be experts for IoT devices. Therefore, they need to be effectively supported when adjusting the entire smart environment to their needs.

6.6 Opportunities for Future Investigations

The bystander view in our study revealed a lack of awareness of the data collection. Bystanders might struggle to judge whether a device is smart. To raise awareness, methods for status communication form an important part of future work. In particular, design solutions for IoT devices with clear status communication should be investigated. Also, other means for raising awareness should be investigated, such as the communication of data collection by information sources different from the smart device. Awareness of the device's status, however, is not sufficient, bystanders need means that support them in finding out where their data is stored, how long it is stored and who has access to it.

When being aware of the data collection, bystanders require means to exert control over it. Future studies should investigate such means and their impact on the owner of the device and further bystanders. In particular, it should be investigated how bystanders can express their preferences to the smart environment and the extent to which this can be performed automatically.

Participants in our studies named different measures that they would take to protect their privacy. The specific impact of those measures on other persons is unclear. Therefore, the effectiveness, as well as the impact of privacy-preserving behavior, should be investigated. Even if owners realize a privacy violation rooted in the output of an IoT device, it is unclear if they act and how. Thus, future studies should investigate means for device owners to adjust the output in the presence of bystanders. We interviewed participants and did not observe their behavior. We consider a field study of privacy violations that result from the presence of bystanders and the real behavior of people of great importance. This is based on statements from our participants that mention that they are uncertain whether they would take the measure in reality. We furthermore did not interview the bystander group of children that live in a smart environment. Since their privacy perceptions might differ from their parents [38, 52], their specific perceptions should be investigated.

6.7 Limitations

Finally, we reflect on several limitations of our work. We interviewed rather young participants that gained familiarity with IoT devices during our study. While this reflects the bystander scenario, it cannot provide insights on frequent visits to smart environments. Future studies should extend both views considering an older sample. We deliberately limited the devices that we investigated in our study to those that are already available on the market. Most of the devices are rather obvious. Future IoT devices might be more unobtrusive and discreet and thus result in even more awareness issues. Thus, future studies should investigate unobtrusive and discreet devices. We conducted a qualitative study which based on its nature does not provide quantitative conclusions. Thus, our work serves as a stepping stone for investigating privacy violations and concerns that arise from the presence of bystanders in smart environments. Future studies should shed light on the quantitative aspects of the investigated views.

7 CONCLUSION

The market for IoT devices is growing. Alongside with benefits offered by such devices, new privacy risks are introduced into the users' homes. This does not only concern the user of the smart home device but also *any* person that is present in the smart home environment. Therefore, the presence of bystanders can result in privacy violations: the privacy of the bystander might be affected by the data collection in their surroundings and the user's privacy might be affected by the bystander observing the output of devices. Our work aimed to shed light on these potential privacy violations conducting in-depth interviews with 42 participants. From our findings, we learn that bystanders are concerned about data collection in their surroundings. They wish to be aware of it and to control the data collection but struggle to gain awareness and to exert control. Users, on the other hand, more often consider convenience and access to information than bystanders when placing devices in their homes. When confronted with privacy, they express the need for detailed controls to adjust the output. Both views show that bystanders already have to be considered during the design of smart home devices. Our findings lay the groundwork for future studies of bystanders in smart homes. Obvious situations like recordings with cameras do not seem to be problematic, it is the cases in which the status or even the existence of a device cannot be judged. Thus, the increasing number of IoT devices and their discreetness raise new challenges for the design of future smart environments. We provide specific challenges for the design for the future smart environment based on the results of our studies. We point to a lack of available solutions in existing IoT devices and environments that respect both users and bystanders. If only one side is respected the self-determination of the other is fundamentally reduced and the reaction will be "I don't know how to protect myself". Future works should address this gap by providing scalable solutions that reduce the burden from users and bystanders by for instance automation or delegation.

ACKNOWLEDGMENTS

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 Horst Görtz Foundation, by the BMBF and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE, JST CREST Grant No. JPMJCR16E1 Experiential Supplements, and by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – 251805230/GRK 2050.

REFERENCES

[1] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Proceedings of the 2019 SOUPS Fifteenth Symposium on Usable Privacy and Security*. USENIX Association, Berkeley, CA, USA, 1–16.

[2] Tousif Ahmed, Roberto Hoyle, Patrick Shaffer, Kay Connelly, David Crandall, and Apu Kapadia. 2017. Understanding Physical Safety, Security, and Privacy Concerns of People with Visual Impairments. *IEEE Internet Computing* 21, 3 (May/June 2017), 56–63. https://doi.org/10.1109/MIC.2017.77

[3] Tousif Ahmed, Apu Kapadia, Venkatesh Potluri, and Manohar Swaminathan. 2018. Up to a Limit? Privacy Concerns of Bystanders and Their Willingness to Share Additional Information with Visually Impaired Users of Assistive Technologies. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)* 2, 3, Article 89 (Sept. 2018), 27 pages. https://doi.org/10.1145/3264899

[4] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 2 (2018), 59. https://doi.org/10.1145/3214262

[5] Patrick Bader, Alexandra Voit, Huy Viet Le, Niels Henze, Albrecht Schmidt, et al. 2019. WindowWall: Towards Adaptive Buildings with Interactive Windows as Ubiquitous Displays. *ACM Transactions on Computer-Human Interaction (TOCHI)* 26, 2 (2019), 11.

[6] Ann Blandford, Dominic Furniss, and Stephann Makri. 2016. *Qualitative HCI research: Going behind the scenes*. Vol. 9. Morgan & Claypool Publishers, Williston, VT, US. 1–115 pages.

[7] Denys Brand, Florence D. DiGennaro Reed, Mariah D. Morley, Tyler G. Erath, and Matthew D. Novak. 2019. A Survey Assessing Privacy Concerns of Smart-Home Services Provided to Individuals with Disabilities. *Behavior Analysis in Practice* 13 (2019), 11–21. https://doi.org/10.1007/s40617-018-00329-y

[8] Nico Castelli, Corinna Ogonowski, Timo Jakobi, Martin Stein, Gunnar Stevens, and Volker Wulf. 2017. What Happened in My Home?: An End-User Development Approach for Smart Home Data Visualization. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 853–866. https://doi.org/10.1145/3025453.3025485

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

[10] Soumyadeb Chowdhury, Md Sadek Ferdous, and Joemon M. Jose. 2016. Bystander Privacy in Lifelogging. In *Proceedings of the 30th International BCS Human Computer Interaction Conference: Companion Volume* (Poole, United Kingdom) *(HCI '16)*. BCS Learning & Development Ltd., Swindon, UK, Article 15, 3 pages. https://doi.org/10.14236/ewic/HCI2016.62

[11] Hyunji Chung, Michaela Iorga, Jeffrey Voas, and Sangjin Lee. 2017. Alexa, Can I Trust You? *Computer* 50, 9 (2017), 100–104.

[12] Mary J. Culnan and Pamela K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization science* 10, 1 (1999), 104–115. https://doi.org/10.1287/orsc.10.1.104

[13] Jaybie A. de Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. 2018. Security and Privacy Approaches in Mixed Reality: A Literature Survey. Cryptology ePrint Archive, Report 1802.05797. , 40 pages. https://arxiv.org/pdf/1802.05797.pdf.

[14] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, New York, NY, USA, 2377–2386.

[15] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In *Proceedings of the 2017 SOUPS Symposium on Usable Privacy and Security*. USENIX Association, Berkeley, CA, USA, 399–412.

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

[17] Nathaniel Fruchter and Ilaria Liccardi. 2018. Consumer Attitudes Towards Privacy and Security in Home Assistants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (Extended Abstracts)*. ACM, New York, NY, USA, LBW050. https://doi.org/10.1145/3170427.3188448

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

[19] Christine Geeng and Franziska Roesner. 2019. Who's In Control? Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. ACM, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300498

[20] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior. *Computers & Security* 77 (2018), 226–261.

[21] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. 2018. Home Sweet Home? Investigating Users' Awareness of Smart Home Privacy Threats. In *Proceedings of the WSSP Workshop on the Human aspects of Smarthome Security and Privacy*. USENIX Association, Berkeley, CA, USA, 1–4.

[22] Marco Ghiglieri, Melanie Volkamer, and Karen Renaud. 2017. Exploring Consumers' Attitudes of Smart TV Related Privacy Risks. In *Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, Cham, Switzerland, 656–674.

[23] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy Behaviors of Lifeloggers Using Wearable Cameras. In *Proceedings of the ACM UbiComp International Joint Conference on Pervasive and Ubiquitous Computing* (Seattle, Washington) *(UbiComp '14)*. ACM, New York, NY, USA, 571–582. https://doi.org/10.1145/2632048.2632079

[24] Timo Jakobi, Corinna Ogonowski, Nico Castelli, Gunnar Stevens, and Volker Wulf. 2017. The Catch(Es) with Smart Home: Experiences of a Living Lab Field Study. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. ACM, New York, NY, USA, 1620–1633. https://doi.org/10.1145/3025453.3025799

[25] Marion Koelle, Matthias Kranz, and Andreas Möller. 2015. Don'T Look at Me That Way!: Understanding User Attitudes Towards Data Glasses Usage. In *Proceedings of the 2015 17th International MobileHCI Conference on Human-Computer Interaction with Mobile Devices and Services* (Copenhagen, Denmark) *(MobileHCI '15)*. ACM, New York, NY, USA, 362–372. https://doi.org/10.1145/2785830.2785842

[26] Marion Koelle, Katrin Wolf, and Susanne Boll. 2018. Beyond LED status lights-design requirements of privacy notices for body-worn cameras. In *Proceedings of the Twelfth International Conference on Tangible, Embedded, and Embodied*

Interaction. ACM, New York, NY, USA, 177–187.

[27] Thomas Kubitza, Alexandra Voit, Dominik Weber, and Albrecht Schmidt. 2016. An IoT Infrastructure for Ubiquitous Notifications in Intelligent Living Environments. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct* (Heidelberg, Germany) *(UbiComp '16)*. ACM, New York, NY, USA, 1536–1541. https://doi.org/10.1145/2968219.2968545

[28] J. Sathish Kumar and Dhiren R. Patel. 2014. A Survey on Internet of Things: Security and Privacy Issues. *International Journal of Computer Applications* 90, 11 (2014), 20–26.

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

[30] Marc Langheinrich. 2002. A privacy awareness system for ubiquitous computing environments. In *international conference on Ubiquitous Computing*. Springer, Cham, Switzerland, 237–245.

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

[32] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2018. Towards security and privacy for multi-user augmented reality: Foundations with end users. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, Piscataway, NJ, USA, 392–408.

[33] Seonglim Lee, Na Eun Park, and Jaehye Suk. 2019. The Effects of Consumers' Information Security Behavior and Information Privacy Concerns on Usage of IoT Technology. In *Proceedings of the XX International Conference on Human Computer Interaction*. ACM, New York, NY, USA, 54.

[34] Christoph Lutz, Christian Pieter Hoffmann, Eliane Bucher, and Christian Fieseler. 2018. The role of privacy concerns in the sharing economy. *Information, Communication & Society* 21, 10 (2018), 1472–1492.

[35] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15, 4 (2004), 336–355. https://doi.org/10.1287/isre.1040.0032

[36] Davit Marikyan, Savvas Papagiannidis, and Eleftherios Alamanos. 2019. A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change* 138 (2019), 139–154.

[37] Terence V. McCann and Eileen Clark. 2003. Grounded Theory in Nursing Research: Part 1 – Methodology. (2003).

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

[39] Sarah Mennicken, David Kim, and Elaine May Huang. 2016. Integrating the Smart Home into the Digital Calendar. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. ACM, New York, NY, USA, 5958–5969. https://doi.org/10.1145/2858036.2858168

[40] Mateusz Mikusz, Steven Houben, Nigel Davies, Klaus Moessner, and Marc Langheinrich. 2018. Raising Awareness of IoT Sensor Deployments. In *Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT*. IET, London, UK, 8. https://doi.org/10.1049/cp.2018.0009

[41] Vivian Genaro Motti and Kelly Caine. 2015. Users' Privacy Concerns About Wearables. In *Proceedings of the 2015 FC International Conference on Financial Cryptography and Data Security*. Springer, Cham, Switzerland, 231–244. https://doi.org/10.1007/978-3-662-48051-9_17

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

[43] Briony J. Oates. 2005. *Researching Information Systems and Computing*. Sage.

[44] Xinru Page, Paritosh Bahirat, Muhammad I. Safi, Bart P. Knijnenburg, and Pamela Wisniewski. 2018. The Internet of What? Understanding Differences in Perceptions and Adoption for the Internet of Things. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 4, Article 183 (Dec. 2018), 22 pages. https://doi.org/10.1145/3287061

[45] Alfredo Perez, Sherali Zeadally, Luis Matos Garcia, Jaouad Mouloud, and Scott Griffith. 2018. FacePET: Enhancing Bystanders' Facial Privacy with Smart Wearables/Internet of Things. *Electronics* 7, 12 (2018), 379.

[46] Sarah Pidcock, Rob Smits, Urs Hengartner, and Ian Goldberg. 2011. Notisense: An Urban Sensing Notification System to Improve Bystander Privacy. In *Proceedings of the 2011 2nd International Workshop Sensing Applications on Mobile Phones*. 1–5.

[47] Blaine A. Price, Avelie Stuart, Gul Calikli, Ciaran Mccormick, Vikram Mehta, Luke Hutton, Arosha K. Bandara, Mark Levine, and Bashar Nuseibeh. 2017. Logging You, Logging Me: A Replicable Study of Privacy and Sharing Behaviour in Groups of Visual Lifeloggers. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1, 2, Article 22 (June 2017), 18 pages. https://doi.org/10.1145/3090087

[48] Olivia K Richards. 2019. Family-Centered Exploration of the Benefits and Burdens of Digital Home Assistants. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, SRC11.

[49] Tom A. Rodden, Joel E. Fischer, Nadia Pantidi, Khaled Bachour, and Stuart Moran. 2013. At Home with Agents: Exploring Attitudes Towards Future Smart Energy Infrastructures. In *Proceedings of the 2013 SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI '13)*. ACM, New York, NY, USA, 1173–1182. https://doi.org/10.1145/2470654.2466152

[50] Statista. 2019. Smart Home Worldwirde. https://www.statista.com/outlook/279/100/smart-home/worldwide (Accessed January 2020).

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

[52] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders Versus Intrusiveness: Teens' and Parents' Perspectives on Home-entryway Surveillance. In *Proceedings of the 2014 UbiComp ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Seattle, Washington). ACM, New York, NY, USA, 129–139. https://doi.org/10.1145/2632048.2632107

[53] Alexandra Voit, Dominik Weber, and Niels Henze. 2018. Qualitative Investigation of Multi-Device Notifications. In *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers* (Singapore, Singapore) *(UbiComp '18)*. ACM, New York, NY, USA, 1263–1270. https://doi.org/10.1145/3267305.3274117

[54] Dominik Weber, Alexandra Voit, Jonas Auda, Stefan Schneegass, and Niels Henze. 2018. Snooze!: Investigating the User-Defined Deferral of Mobile Notifications. In *Proceedings of the 20th MobileHCI International Conference on Human-Computer Interaction with Mobile Devices and Services*. ACM, New York, NY, USA, 2. https://doi.org/10.1145/3229434.3229436

[55] Dominik Weber, Alexandra Voit, Gisela Kollotzek, Lucas van der Vekens, Marcus Hepting, Florian Alt, and Niels Henze. 2018. PD Notify: Investigating Personal Content on Public Displays. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI EA '18)*. ACM, New York, NY, USA, Article LBW014, 6 pages. https://doi.org/10.1145/3170427.3188475

[56] Katrin Wolf, Karola Marky, and Markus Funk. 2018. We should start thinking about Privacy Implications of Sonic Input in Everyday Augmented Reality!. In *Mensch und Computer 2018 - Workshopband*. Gesellschaft für Informatik e.V., Bonn, Germany, 353–359. https://doi.org/10.18420/muc2018-ws07-0466

[57] Peter Worthy, Ben Matthews, and Stephen Viller. 2016. Trust Me: Doubts and Concerns Living With the Internet of Things. In *Proceedings of the 2016 DIS ACM Conference on Designing Interactive Systems*. ACM, New York, NY, USA, 427–434. https://doi.org/10.1145/2901790.2901890

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

[59] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–24.

[60] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security & Privacy Concerns with Smart Homes. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Berkeley, CA, USA, 65–80.

[61] Eric Zeng and Franziska Roesner. 2019. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study. In *Proceedings of the 28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Berkeley, CA, USA, 159–176.

[62] Yu Zhai, Yan Liu, Minghao Yang, Feiyuan Long, and Johanna Virkki. 2014. A Survey Study of the Usefulness and Concerns About Smart Home Applications From the Human Perspective. *Open Journal of Social Sciences* 2, 11 (2014), 119. https://doi.org/10.4236/jss.2014.211017

[63] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW, Article 200 (2018), 20 pages. https://doi.org/10.1145/3274469

[64] Verena Zimmermann, Merve Bennighof, Miriam Edel, Oliver Hofmann, Judith Jung, and Melina von Wick. 2018. 'Home, Smart Home'–Exploring End Users' Mental Models of Smart Homes. In *Mensch und Computer 2018-Workshopband*. Gesellschaft für Informatik e.V., Bonn, Germany, 407–417.

[65] Verena Zimmermann, Paul Gerber, Karola Marky, Leon Böck, and Florian Kirchbuchner. 2019. Assessing Users' Privacy and Security Concerns of Smart Home Technologies. *i-com – Journal of Interactive Media* 18, 3 (2019), 197–216. https://doi.org/10.1515/icom-2019-0015