Roles Matter! Understanding Differences in the Privacy Mental Models of Smart Home Visitors and Residents

KAROLA MARKY*, University of Glasgow, United Kingdom and Technical University of Darmstadt, Germany
SARAH PRANGE*, Bundeswehr University Munich, Germany and LMU Munich, Germany
MAX MÜHLHÄUSER, Technical University of Darmstadt, Germany
FLORIAN ALT, Bundeswehr University, Germany

In this paper, we contribute an in-depth study of the mental models of various roles in smart home ecosystems. In particular, we compared mental models regarding data collection among residents (primary users) and visitors of a smart home in a qualitative study (N=30) to better understand how their specific privacy needs can be addressed. Our results suggest that visitors have a limited understanding of how smart devices collect and store sensitive data about them. Misconceptions in visitors' mental models result in missing awareness and ultimately limit their ability to protect their privacy. We discuss the limitations of existing solutions and challenges for the design of future smart home environments that reflect the privacy concerns of users and visitors alike, meant to inform the design of future privacy interfaces for IoT devices.

CCS Concepts: • **Human-centered computing** → **Ubiquitous and mobile devices**; User studies; • **Security and privacy** → *Usability in security and privacy*.

Additional Key Words and Phrases: Bystander Privacy, IoT Devices, Smart Homes

ACM Reference Format:
Karola Marky, Sarah Prange, Max Mühlhäuser, and Florian Alt. 2021. Roles Matter! Understanding Differences in the Privacy Mental Models of Smart Home Visitors and Residents. In *20th International Conference on Mobile and Ubiquitous Multimedia (MUM 2021), December 5–8, 2021, Leuven, Belgium.* ACM, New York, NY, USA, 25 pages. https://doi.org/10.1145/3490632.3490664

1 INTRODUCTION

The share of smart devices in private households has been steadily increasing in the past years [59]. Smart home devices are specifically designed to facilitate users' daily life. They can enhance the convenience of everyday life, for instance, through automation or by providing better control of energy consumption [40].

To provide their functionality, smart home devices collect and store data about users and their environment. Despite the obvious benefits, collecting and processing data raises privacy and security concerns of (potential) smart home users. These concerns have repeatedly been studied in the literature (cf. [69, 72, 74]). However, prior work strongly focused on *residents*, i.e. those living in the smart home who own and control the devices.

At the same time, smart home devices collect, store, and process data, independent of *who* is present and might be affected. As a result, *bystanders*, in particular *visitors* of smart homes, are typically either unaware of smart home devices

*Both authors contributed equally to this research.

Manuscript submitted to ACM

collecting and using data about them and/or have little to no means to influence which data is collected about them and when [33, 41, 42, 52, 68]. Prior work showed that visitors wish to limit data sharing in foreign smart homes [19, 41, 42] and recommended to design devices that provide visitor modes [33, 42, 69, 70], to investigate options for making smart devices discoverable [54, 58], or to provide means for visitors to exert control over the data that is collected about them [41, 68].

What remains mostly unexplored though, is whether and to what degree visitors *understand* how smart devices affect their privacy. This knowledge is yet crucial to design appropriate solutions. To close this gap, we specifically focus on the perspectives of smart home residents and visitors as well as the interplay of both roles. We answer the following research questions:

RQ1 What are common *privacy perceptions* of *residents* and *visitors* regarding smart home ecosystems?
RQ2 What are *misconceptions* of *residents* and *visitors* regarding privacy in the smart home data ecosystem?
RQ3 What are *differences* in privacy perceptions of *residents* and *visitors* regarding smart home ecosystems?

We contribute an in-depth investigation of the privacy mental models of two roles in smart home ecosystems (i.e., residents and visitors). We invited 30 participants (15 per role) to participate in a drawing exercise. The participants were asked to illustrate their mental models of data creation, flow, and storage in smart home ecosystems. The drawing exercise was complemented by semi-structured interviews. Participants in the resident perspective were asked about their own experiences with smart home devices, while those in the visitor perspective were asked about experiences while visiting other smart homes.

We found that residents generally have a more detailed understanding of data collected about them in smart home ecosystems with fewer misconceptions than visitors. Furthermore, misconceptions in the visitors' privacy mental models prevent them from acting in a way that matches their privacy needs and are independent of their technical understanding of the data flow in the smart home ecosystem. For instance, visitors often believed that active interaction or registration with a smart device (e.g., a smart doorbell) is necessary for it to collect and process sensitive data about them. We discuss the limitations of existing solutions that aim to support the privacy decisions of residents and visitors. We conclude with identifying challenges for the design of privacy interfaces for smart home scenarios respecting both roles, discuss opportunities to address these, and provide directions for future research.

2 BACKGROUND AND RELATED WORK

To set the scene for our work, we draw from several strands of research, namely work on *smart home ecosystems* and *mental models* in general, prior work on *perceptions of smart home privacy*, and *bystander privacy*.

2.1 Smart Home Ecosystems

Smart homes have been described in the literature as households equipped with various devices offering computing power and serving various purposes, such as promoting comfort, security, and entertainment [4, 7, 22], aiming at providing a convenient living environment for users [57]. Smart home devices are typically equipped with sensors to gather data about users and their environments (potentially being stored and processed outside the smart home) [25], and connected to each other, to the Internet and/or the provider [55]. An increasing variety of smart devices is commercially available [59]. Devices come in various form factors [55] and support various application cases, such as increasing comfort by automation and remote control; monitoring health data via diverse senors; and sustainable energy consumption [40]. At the same time, these raise new challenges for usable privacy and security [5].

Overall, work evolves around smart homes and their benefits, interaction with smart devices, adoption, concerns, and sharing of IoT devices [23, 53]. Marikyan *et al.* identified user perceptions as an open direction for future research, suggesting to further investigate various stakeholders' perceptions [40].

2.2 Mental Models

Mental models are internal representations humans derive from the real world [29]. Based on mental models, humans adapt their behavior. The level of sophistication of mental models differs between individuals [8, 29, 30]. When using technologies, users can have two types of mental models: 1) functional and 2) structural models [49]. Users with *functional* models know how to use a technology, but not how the technology works in detail. Users with *structural* models have a detailed understanding of how a technology works. This also implies that mental models must be sound enough for users to interact with a technology [34]. Once a mental model has been constructed, it is rarely modified [62]. Misconceptions in mental models might lead users to behaviors that do permanently not represent their actual needs.

2.3 Perceptions of Smart Home Privacy

In general, privacy is users' possibility to control the conditions under which their personal data is captured and processed by a third party [16]. This means that privacy is individually defined by each user. Smart home devices collect and process data about users and their environments. The perceptions and mental models of users regarding this data collection have been studied by a plethora of works [2, 6, 9, 11, 13, 19, 64, 66, 69, 71]. Mental models for specific devices, such as smart speakers, have been investigated considering respective privacy risks within a (shared) household scenario [27]. Many of these identified privacy concerns and barriers that hinder people from becoming smart home users. The data collection by smart home devices has repeatedly been identified as a major privacy concern [1, 61, 67].

When asked for specific concerns and consequences from privacy invasions, participants frequently named the physical security of their homes and the possibility for hackers to gain access to smart home devices via the Internet [69, 74]. Hence, smart home users wish to be aware of the specific data that is collected and transferred to providers [19, 28, 45] or data should be anonymized [35]. At the same time, there are several reasons for which users are willing to sacrifice privacy. Among those, convenience constitutes a primary factor for adopting smart home technologies and for disregarding personal privacy concerns [19, 72]. However, these studies mostly focused on primary users and/or shared household scenarios, rather than considering external bystanders such as visitors.

2.4 Bystander Privacy

The privacy of bystanders has been studied in related domains, such as life-logging [26, 32, 48] and augmented or mixed reality [3, 12, 17, 37, 46, 51, 65]. All of these works show that bystanders wish to be aware of their data being recorded to make the decision whether or not to share this data.

Prior work on smart homes focused on people beyond primary users includes investigations of privacy concerns among minors [43, 44, 56, 63]. Parents have to consider a trade-off between knowing about their children's actions and their children's privacy. Other work investigated multi-user scenarios in smart homes with multiple residents, showing that on one hand privacy can be negotiated among them [24], but that on the other hand, social relations make this difficult at times [67]. Visitor modes for smart homes, that provide visitors with functionality while still preserving the owners' privacy, have been suggested [70]. Naeini *et al.* investigated the willingness to share data in spaces equipped with smart devices [19]. Among other scenarios not related to bystanders, they investigated the visit of a friend's smart home with a presence sensor to control lights. Their results show that users find data sharing in

public places (e.g., a department store) more acceptable than in private ones (e.g., a friend's home). This indicates that bystanders in private places might not accept their data to be shared. Yao *et al.* studied bystander privacy in smart homes in three scenarios [68], each investigating a specific smart home device in a co-design study. 18 participants identified factors that impact and mitigate their concerns. Most importantly, bystanders wish to exert control over data collection, also by interacting with the smart home device themselves. Similarly, Marky *et al.* investigated bystander privacy in scenarios that represented different levels of familiarity with the smart environment [41]. They found that bystanders exhibit several misconceptions about their privacy. Mare *et al.* specifically investigated perceptions of smart devices in AirBnBs [39]. Further research investigated means to support the discoverability of smart devices in environments that are private and at the same time unknown to visitors, such as hotel rooms. A combination of LED indicator lights and a beep sound can support users in discovering devices [58]. Another suggestion is to visualise spaces of data collection by means of augmented reality [54]. More general studies about smart home visits showed that bystanders have difficulties to protect their privacy in foreign smart homes because of a lack of strategies [42]. While individuals would use technological solutions, communication with the device owners was overall considered as appropriate solution to address privacy needs of visitors [14].

2.5 Summary

Smart devices affect not only single users but also bystanders in environments where multiple people can be present. Prior work investigated *multi-user* scenarios, where all users are residents of the smart home, and considered the perceptions of bystanders and primary users separately. However, visiting a smart home differs from such multi-user scenarios as IoT devices can capture data without explicit interaction. Several *misconceptions and awareness issues* were identified in prior work.At the same time, mental models help users assessing whether their privacy is violated in smart homes. Misconceptions within these models can prevent users from acting according to their privacy needs.

In this paper, we specifically investigate privacy mental models of the smart home ecosystem for two roles of smart home residents and visitors, as these have not been well understood as of today. This allows us to compare them, investigate the origin of misconceptions, and to draw conclusions that support better design of future smart home environments and their privacy mechanisms that address the needs of both roles.

3 METHODOLOGY

To investigate the mental models of *visitors* in smart home ecosystems, we conducted two studies – one with visitors and one with *residents* – as basis for a comparison. The study for each targeted role was split into two parts: 1) a drawing exercise in which we asked participants to sketch their mental models and 2) a semi-structured interview to obtain a deeper understanding. Drawing exercises are effective to capture the mental models of users considering specific systems or technologies [30, 69, 73]. We further opted for semi-structured interviews since they offer a certain structure while at the same time providing enough freedom to investigate participants' perceptions in depth [50]. To inform the interview guide, we conducted one exploratory interview per targeted role. Further pilot tests helped improve question clarity. Results from the pilots are not reported.

3.1 Procedure

The procedure was identical for both targeted roles. However, we adapted the questions and the scenario to match the respective role. All sessions were audio-recorded, while the drawing process was also video-recorded. A session lasted

approximately one hour in total. We deliberately did not mention "privacy" in the study invitation, nor the consent form or interview questions to avoid priming. The detailed procedure was as follows (cf. Figure 1):

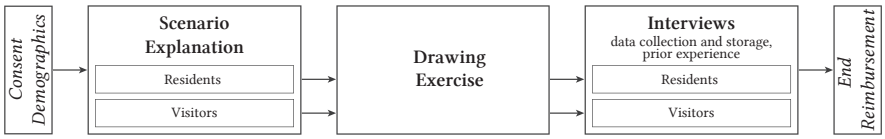


Fig. 1. Schematic depiction of our study procedure.

1) Consent and Demographics. We commenced by providing participants a consent form which we asked them to sign. Next, participants provided demographics, including their living situation, employment status, affinity for technology following the ATI scale [21], and experiences with the usage of smart devices. We included the 10-item IUIPC [38] to assess participants' privacy perception prior to the study.

2) Drawing Exercise. We introduced participants to the scenario to nudge them to think based on their role. Residents were asked to consider devices that they use at their home while visitors were asked to consider visiting the smart home of another person. Then, participants conducted the drawing exercise. We provided them with a piece of paper in DIN A3 size and pens in different colors.

Participants in prior studies including a drawing exercise (cf. [73]) faced two challenges. First, it was difficult for them to add details to their sketches resulting in very simple sketches. Second, the participants struggled in commencing with sketching. To mitigate these issues, we provided a wide range of printed cut-outs of smart home devices that the participants could choose for their sketches. We furthermore wanted to ensure that participants indeed consider a smart home ecosystem as a whole. In particular, we asked them to choose devices of five categories of smart home devices that are already available on the market (at least one each). Those categories were: 1) entertainment and communication, 2) energy management, 3) security and safety, 4) health and 5) home automation (cf. Appendix C for the full list of devices). We specifically asked participants to sketch their understanding of how the devices are connected to each other, including their understanding of the data flow with a focus on data that contains personal information about them. During the drawing exercise, we encouraged participants to think aloud and comment on what they were drawing. Previous studies demonstrated the effectiveness of this combination [69].

3) Semi-Structured Interview. We proceeded with role specific, semi-structured interviews. We used the sketch from the previous part as the basis for the discussion. Participants were instructed to highlight devices and entities that collect or receive data about them and explain their understanding of it. Next, the examiner asked participants to label entities in their sketches to clarify them.

4) End and Reimbursement. After the interview, we gave participants the opportunity to ask questions or to provide additional feedback. Finally, we reimbursed them with an online shopping voucher valued at roughly 10 dollars.

3.2 Participants and Recruitment

We recruited 30 participants (15 residents, 15 visitors) via mailing lists, flyers, poster advertisements, and social networks. We aimed at recruiting participants with different experiences regarding smart home devices in order to capture a wide range of possible mental models. Considering the resident role, we invited participants that either already own smart home devices or are interested in buying devices soon. We did not apply restrictions to the visitor role.

3.2.1 Demographics. Participants' age ranged from 18 to 64 ($MN = 30.33$, $SD = 12.12$), $N = 7$ identified as female, most of them were students ($N = 18$), and living with their family ($N = 10$). By means of the ATI scale [21], we assessed participants' affinity for technology on a scale from 1 to 6, where higher values indicate a higher affinity for technology. Residents' ATI ranged from 2 to 5.78 ($MN = 4.06$, $SD = 1.04$), visitors' ATI was similar and ranged from 2.78 to 5.56 ($MN = 4.33$, $SD = 0.66$). Table 1 provides an overview of our sample. Table D (Appendix) shows details per participant.

3.2.2 Prior Experiences with Smart Devices. Within the demographics questionnaire, we asked participants to list their own smart home devices, if applicable. Furthermore, we asked them about prior experiences and how often they interacted with smart devices (at home and in general) in the semi-structured interview.

Overall, ten participants (residents: 6, visitors: 4) reported owning smart devices[1]. Of them, three participants in the resident role and one in the visitor role had multiple smart home devices that are connected to each other.

Table 1. Participants' demographics, employment status, and ATI scale, for residents, visitors and both.

		Residents	Visitors	Sum
Age	Mean	35.73	24.93	30.33
	SD	15.29	2.84	12.12
Gender	male	12	11	23
	female	3	4	7
	prefer not to say	0	0	0
	other	0	0	0
Work	student	7	11	18
	self-employed	3	0	3
	employed full time	0	3	3
	other	5	1	3
ATI Scale	Min	2.00	2.78	2.00
	Max	5.78	5.56	5.78
	Mean	4.06	4.33	4.19
	SD	1.04	0.66	0.86

Participants reported on *further* experiences with smart home devices, including visits of smart homes (residents: 2, visitors: 11), or having shared a device (e.g., in their flatshare, visitors: 2).

3.2.3 Privacy Perceptions. To assess participants' privacy perception, we applied the 10-item IUIPC questionnaire [38]. Higher values in the IUIPC scales indicate that participants are more sensitive regarding privacy concerns. Overall, they rated their wish to exert *Control* with $Mean = 6.07$ (residents: 6.15, visitors: 6.00), their *Awareness* about privacy practices with $Mean = 6.1$ (residents: 6.2, visitors: 6.00), and the perceived ratio between *Collection* and benefits with $Mean = 5.38$ (residents: 5.42, visitors: 5.33, refer to Table 3 in Appendix B for detailed values).

3.3 Ethical Considerations

With our study, we followed the guidelines of the ethics committees at the authors' institutions. User studies at our institutions have to limit the collection of personal data in order to preserve participants' privacy. Each participant received a randomly assigned identifier. Prior to the interview, each participant signed a consent form. The consent form was stored separately from all other data such that data cannot be linked to participants' identities. Our institutions are located in a country without a requirement for following a formal IRB process for the kind of user study we conducted. Still, we took the necessary precautions to preserve participants' privacy. Note that we conducted the interviews prior to the COVID-19 pandemic.

[1]Note, that in case only the smartphone was mentioned (questionnaire and/or interview), we did not count it as it is not a standalone smart home device, but is usually used together with other devices.

3.4 Data Analysis

First, we transcribed the audio recordings and digitized the sketches. Then, we analyzed the sketches and interview transcripts in two sessions using thematic analysis [10]. The analysis consisted of open, axial and selective coding.

In the first session, we analyzed the *level of sophistication* of the mental models expressed in the *sketches*. For this, we followed an open-coding approach in which two authors were coders. In an initial discussion, they developed a code dictionary. The dictionary consisted of four codes for the expressed level of sophistication by reviewing all sketches and by agreeing on a final code dictionary. Then, they independently coded all sketches. Results were discussed and final code allocations for each drawing were agreed upon. Throughout the analysis, we also considered the audio recordings to complement the information expressed in the sketches in cases where parts of the drawing were unclear. To determine the inter-rater reliability, we calculated Cohen's κ, which is 0.824 (almost perfect agreement).

In the second session, we analyzed the *interview transcripts* to develop the mental models of *data collection and storage*. Two researchers individually coded two representative interviews for each view, using thematic analysis with open coding. We then established a coding tree in a review meeting and applied it to the remaining interview transcripts. The coding tree consists of 103 codes. We related those codes to each other by using axial coding which resulted in six final categories of codes. Through selective coding, we removed codes without sufficient data to be considered as robust, such as codes which were used only once over all participants. The full coding tree is available in Appendix A.

Finally, based on the codes from the transcript analysis and the level of sophistication, we developed participants' mental models of the smart home ecosystem, including their perception of entities that capture and store personal data.

3.5 Limitations

Due to the qualitative nature of our study, quantitative conclusions cannot be made. We provided our participants with printed pictures from smart home devices to support them during the drawing exercise, which might have had an impact on their drawings. However, in order not to limit them in their expression, we provided products that are already available on the market from a wide range of product categories. To create a list of available devices, we systematically searched best-seller lists of online stores resulting in a list of 89 smart home devices. We grouped similar devices and provided a generic depiction as print out to the participants. Not to limit them in their drawing, we also told them that they could add devices if they are not present as print-out.

Our sample consists of participants with a mean age of 30.33 years. While the usage of smart homes is dominant within this age group in Germany [60], our sample might not be representative. Furthermore, 18 of 30 participants were students and many were living with their family (10) or partner (9). Hence, our results may only apply to users with a similar background.

4 RESULTS

In this section, we illustrate the findings of our study. First, we provide a descriptive overview of the *content and topology* of the participants' sketches showing the devices and additional entities they incorporated. Then, we present the mental models on the *smart home ecosystem*, *data collection*, and *data storage*. We cite residents as P_R (N_R for descriptive counts) and visitors as P_V (N_V).

Table 2. Overview of additional entities: participants added various entities to their sketches (N_R: counts for residents, N_V: visitors).

		N_R	N_V	Sum
Objects & Setting	Router	6	3	9
	Homes / Houses / Rooms	2	2	4
	Additional Smart Devices	6	11	17
Abstract Entities	Apps & Services	5	0	5
	Companies & Providers	9	2	11
	Cloud	3	2	5
	Internet	5	5	10
Threats	Hackers	2	0	2
	digital footprint	1	0	0
People	User	5	1	6
	Guest	0	3	3

4.1 Content and Topology

In this section, we summarize the content of the participants' sketches. We provide details on the *devices* chosen by the participants, *additional entities* they added to their sketches, and the *topology of the sketches*. This serves as a descriptive overview about what the participants drew.

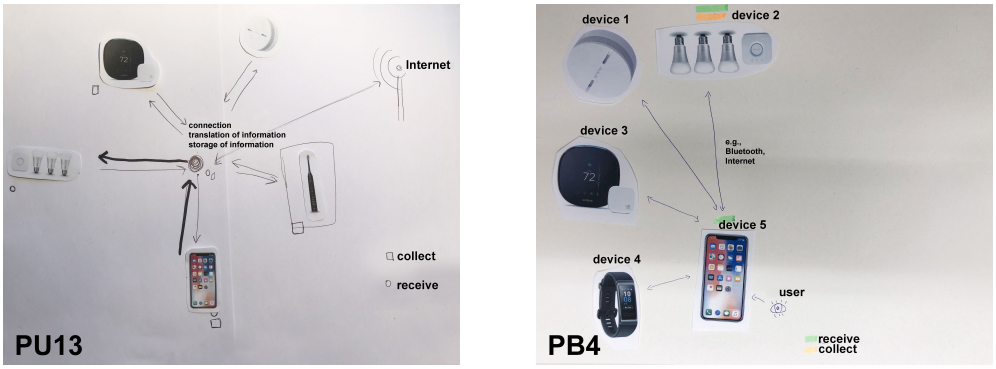
4.1.1 Device Choice. To ensure that participants consider an ecosystem of *different devices*, we asked them to choose one device from each of the following five categories *Entertainment & Communication*, *Energy Management*, *Security & Safety*, *Health*, and *Home Automation*. Participants were free to add further entities and devices. Table 4 in Appendix C provides an overview of available and chosen devices.
In general, participants in the visitor scenario tended to choose devices with which they would interact directly (e.g., the smart doorbell ($N_V = 4$)), while residents rather chose devices that are likely to be used in their home even without a constant direct interaction (e.g., smart heating ($N_R = 4$)). Considering specific devices, both groups mostly added a smartphone for communication ($N_R = 8$, $N_V = 7$), smart lights for energy management ($N_R = 8$, $N_V = 7$), and smartwatches for health ($N_R = 8$, $N_V = 12$) to their sketch. As for security and safety, participants mostly chose a smart smoke detector ($N_R = 5$, $N_V = 5$). For automation, a smart vacuum cleaner was most popular for residents ($N_R = 6$) and smart jalousies or fridges ($N_V = 4$ each) for visitors.

4.1.2 Additional Entities. Participants were not limited to the five chosen devices. All of them added *additional entities* in their sketches (cf. Table 2 for an overview). First, they added physical *objects* and devices (e.g., routers) or set the scene with concrete rooms of their smart home scenario. Second, *abstract entities*, such as service providers, the Internet, or apps were mentioned in some sketches. Third, participants added themselves as *a user*. Finally, some added *potential threats* (such as hackers) to the ecosystem.

4.1.3 Topology of Sketches. All participants except for one resident arranged their sketch around a *central node* which is connected with the majority of devices to control them and/or process and store the data. The central node was either a local server/network or router within the smart home ($N_V = 5$, $N_R = 4$), an external server that is reachable over the Internet ($N_V = 2$, $N_R = 0$), an additional IoT/smart device, such as a smartphone/tablet ($N_V = 5$, $N_R = 8$), the users themselves ($N_R = 2$), a generic/unspecified device ($N_V = 2$, $N_R = 2$) or a smart home app ($N_R = 1$). Note that 2 residents specified both, a router and a smartphone, as central device. Residents stated, e.g.:

> *"And then, they're connected somehow. But I don't know how it gets there."* (P_R8)
>
> *"There is that central component, but I don't know how this is called."* (P_R13)

Comments given by the participants in the visitor target group are:



(a) Schematic Simplification (Primary User) (b) Schematic Simplification (Bystander)

Fig. 2. Participants' sketches showing examples of *schematic simplification* mental models. We replaced participants' notes with digital labels to enhance readability.

> *"A WiFi router or maybe the particular company has its own kind of wireless connector that wirelessly controls all the devices."* (P_V12)
> *"Well, there is the smartphone from which everything can be controlled."* (P_V5)

Furthermore, participants had different understandings of how the entities of the smart home ecosystem can be *connected* to each other. Devices were either connected via a local WiFi network, Bluetooth, or the Internet.

4.2 Level of Detail

Based on the interviews and sketches, we found four types of mental models regarding the smart home ecosystem, differing in their *level of sophistication*. For the individual assignment of each participant to a mental model, refer to Appendix D. Previous work on mental models of smart home users used two levels of sophistication (e.g., [61]). We provide a more nuanced view to demonstrate differences between the investigated target groups of visitors and residents.

(1) **Schematic Simplification.** Some participants in our study illustrated smart home technologies without a detailed understanding, referring to a functional mental model [49]. Accordingly, participants only sketched connections between the devices within the five categories provided by the examiner. These connections were not further specified. The role of external entities, such as the Internet or external service providers, were not explained or not mentioned at all.
For instance, P_R13 in the resident group only connected the five devices with a point in the middle that represents a network between them (see Fig. 2a). Similarly, P_V4 in the visitor group used the smartphone as a central node and sketched simplified connections to the smart home devices, depicting additional entities outside the home (see Fig. 2b). Five visitors and three residents demonstrated this level.

(2) **Basic Understanding.** This type of model is characterized by extending the previous type with external entities, such as the Internet or a cloud as well as a clear connection to them. The basic understanding also forms a functional model [49] since details are very limited.

For instance, P_R2 sketched a basic server as an additional entity and an Internet connection (Fig. 3a). P_V12 drew an external server and a connector within the smart home and different connections between entities (Fig. 3b). Seven visitors demonstrated a basic understanding, and three participants in the resident group.

(3) **Advanced Understanding.** Participants demonstrating an advanced understanding frequently sketched a central component (e.g., a smartphone or server) controlling all other devices. They made a distinction between a local network and the Internet and added other components (e.g., a central server) that go beyond the five categories we provided. This forms a basic structural model since details about the connections and topology are included [49].
P_R3 depicted different types of connections. They made a distinction between data within the smart home and data that leaves it but did not differentiate entities outside the smart home (Fig. 3c). P_V15 drew a similar sketch but included a window and a treadmill within the smart home. Again the entities outside the home were simplified (see Fig. 3d). Six visitors showed an advanced understanding, and five participants in the resident group did.

(4) **High-level Understanding.** The high-level understanding is a sophisticated structural model [49]. The participants made clear distinctions between different network types within and outside the smart home. They added additional entities, such as the Internet, clouds, and even attack surfaces. They also sketched a clear data flow between the devices.
For instance, P_R7 demonstrated a detailed understanding of entities outside the smart home by including entities such as a cloud, different providers, and data types (see Fig. 3e). P_V10 added different providers, a cloud, and the Internet and sketched the connections between the different devices, the possibility to receive updates and how to interact with them as a visitor (see Fig. 3f). One participant in the visitor group showed a high-level understanding and four residents did.

4.3 Data Collection

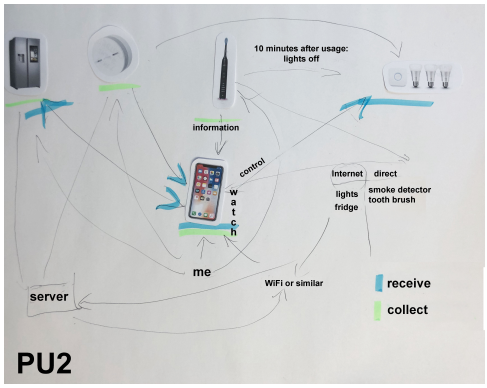
We asked participants to mark devices that *collect* data about them (e.g., new data created by sensors) and to explain how the data collection works according to their understanding. We also asked them to mark devices that *receive* data (e.g., existing data within the ecosystem captured by other devices' sensors) about them and to explain how.

(1) **No interaction, no data collection.** This cluster of mental models describes cases in which no data is collected automatically but only as users directly interact with a smart home device. Six participants in the visitor target group believed that devices do not collect data about them unless they directly interact with the device's interface. Surveillance cameras and motion sensors form an exception. For these, participants understood they only need to be in the vicinity of the devices.

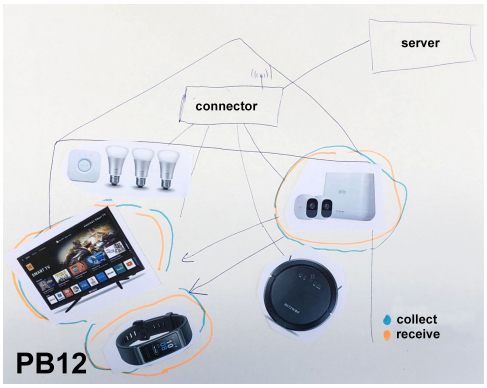
"I also do not know who registers that I am out of the house and what registers that I am out of the house and what registers that the lights are still on, no idea." (P_R13, schematic simplification)

"It depends a lot on the usage. For example, if I would charge my phone and go to the power outlet. But in principle the power outlet could collect data from me [...] I don't wear the smartwatch, Thus I do not think so [that it collects data about me]." (P_V14, basic understanding)

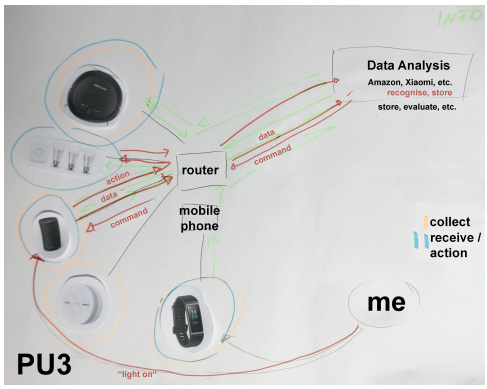
This model was prominent among participants with a functional mental model of the smart home ecosystem, i.e. a schematic simplification or a basic understanding.



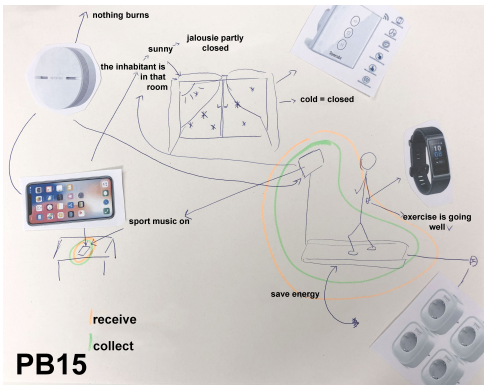
(a) Basic Understanding (Primary User)



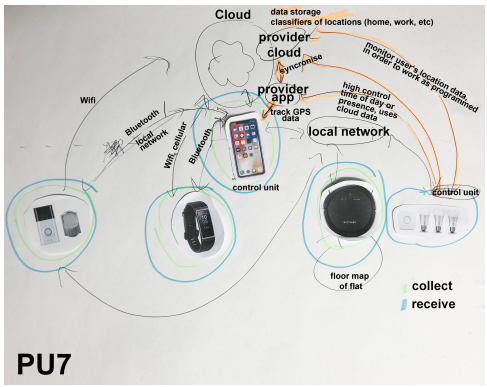
(b) Basic Understanding (Bystander)



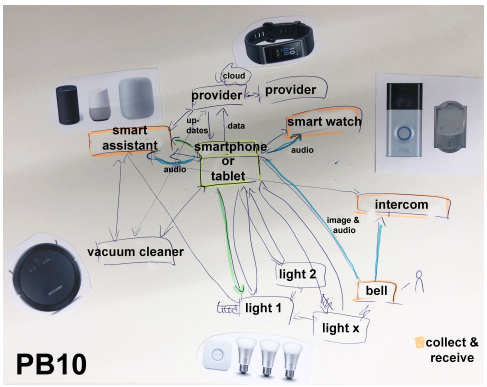
(c) Advanced Understanding (Primary User)



(d) Advanced Understanding (Bystander)



(e) High-level Depiction (Primary User)



(f) High-level Depiction (Bystander)

Fig. 3. Participants' sketches showing examples of *basic*, *advanced*, and *high-level understanding* mental models. We replaced participants' notes with digital labels to enhance readability.

(2) **No registration, no personal data.** Another aspect mentioned by visitors is that even if they interact with a device that captures data, the data is not personal unless they register as users with the specific device. This was mentioned by four participants in the visitor target group, e.g.:

"With the refrigerator, the question is what kind of functionality it has. In principle, if I take a beer out now, it collects data somewhere that at least one beer is missing. It probably can't assign it to me, but it is missing." (P_V14, basic understanding)

"When I sit on the sofa as a guest and switch through the TV, I also generate data. Also not individually, so they can't draw conclusions about me, nevertheless, it generates data of course." (P_V2, advanced understanding)

Again, this type of model was mostly expressed by participants with a rather functional mental model, i.e. a schematic simplification or a basic understanding.

(3) **Known devices form exceptions.** Visitors believed that smartphones collect data about smart home visitors. All participants who explained this aspect connected it to their existing knowledge about and experiences with smartphones:

"With a smartphone, I could imagine the front camera running or anything else being recorded. The moment it is collected, I always assume that it will be stored." (P_V11, schematic simplification)

(4) **All devices collect data, except wearables.** Participants expressed that in general all devices in the vicinity of a person can collect data about them. Wearables, however, form an exception as participants expected that they have to be worn to collect data. Two participants in the visitor target group expressed that all smart home devices collect data about them. They considered the resident's smartwatch as an exception because the visitor is not wearing it, e.g.:

"All except for the smartphone and smartwatch of the owner." (P_V9, basic understanding)

"Generally all [devices] that I've described I would say, except for the smartwatch." (P_V6, basic understanding)

(5) **Local actions without an Internet connection.** When considering the data flow, participants in both groups believed that a connection to the Internet is only required if controlling or accessing data from a device at a remote location but not to trigger a local action.

"I think it is also a simple connection because only mechanically something [the jalousie] goes up and down. Compared to other devices, there is no connection to the Internet in the sense that it is now looking or something special." (P_R5, advanced understanding)

"What I actually think about are light bulbs, but I don't need light bulbs that I have to switch off from outside the house, I just need a light bulb where I don't have to get up from the bed." (P_R12, high-level understanding)

(6) **Configuration by a third party can violate privacy.** Two participants in the visitor group reported negative experiences based on smart devices that were configured by a third party in their own apartment, e.g.:

"My landlord installed a device showing how warm it is in the room and how humid the air was, and said it would be for my own control when I have to ventilate and turn on the heating. [...] Later, I found out that this [device] sent data via WiFi to my landlord's laptop. He actually came up and knocked if it was too warm or too humid or something and told me to air the room. Unpleasant experience." (P_V4, schematic simplification)

4.4 Data Storage

Finally, we assessed mental models on where data collected in smart home environments is *stored*.

(1) **Data is stored locally.** Participants that described this mental model believed that data about them is only stored within the smart home (network). It could be stored on the smart device itself ($N_V = 6$, $N_R = 1$), or on a dedicated storage device ($N_V = 4$, $N_R = 4$).
The following comments were provided by participants in the resident target group:

"I think the [vacuum] robot has its own processing power, it does not need a cloud." (P_R7, high-level)
"The best thing would be to have your own server, where your data [...] is stored, without the data leaking out, without anyone being able to infer consumer behavior from it [...]. Only if you then agree correspondingly, the data may also be used." (P_R15, schematic depiction)

(2) **Data is stored remotely.** Remote storage refers to a cloud server accessible via the internet ($N_V = 2$, $N_R = 3$). Note, that only the smart home user was perceived to have access to it, e.g.:

"On the devices themselves only for a short time, because I assume that not much data can be stored there and that there is no storage capacity, i.e. the data is always deleted. Everything is stored in the cloud." (P_V2, advanced understanding)

(3) **Data is stored remotely by the provider.** In this model, the data is stored in the cloud of the provider of the IoT device ($N_V = 8$, $N_R = 7$), e.g.:

"On a server. Someone is the provider of all of that." (P_V5, advanced understanding)

"[...] I'm scared because I don't know exactly what's going to happen with the data." (P_R14, adv. understanding)

(4) **No knowledge of data storing.** Finally, one participant from the visitor group expressed to have no idea where the data is stored:

"I don't know. I really don't know. I could imagine that there might be local memory for one thing, but probably it will be more like cloud-based external memory. I don't know." (P_V14, basic understanding)

5 DISCUSSION

We now discuss the results of our study. We first describe the difficulty to derive a sound mental model due to the *heterogeneity of smart home ecosystems*. Then, we discuss *differences* and *misconceptions* in the mental models of visitors compared to residents. Next, we discuss *challenges* for the design of privacy mechanisms targeting visitors and suggest *directions for future research*.

5.1 Heterogeneity of Smart Home Ecosystems

The first common theme throughout our results is a difficulty with the heterogeneity of smart homes. While a generic smart home ecosystem can be explained by a simplified depiction, there are a plethora of possibilities to configure specific environments. This results from the large variety of devices on the market. For instance, smart TVs range from simple models with a WiFi connection to more sophisticated models with additional sensors, such as microphones or even cameras. Thus, there is no standard way of abstracting the data collected and stored by an arbitrary smart home device.

Heterogeneity is also reflected by the various connection types and device configurations participants sketched. This indicates that it is difficult to judge whether a device collects data without prior knowledge making it particularly difficult to derive a sound mental model of a specific smart home, especially for visitors. Participants in both roles correctly depicted the data flow of specific devices that they had prior knowledge of, for example, Amazon Echos. Furthermore, the data captured by smartphones was depicted accurately. This might result from most smartphones sharing a common set of sensors and being well-known to participants. As a result, a mental model being correct for one smart home might be wrong for another. However, known devices were depicted accurately.

Prior work has also shown that once established, existing mental models are difficult to change [62]. Hence, residents or visitors with pre-existing mental models of privacy-respecting smart home ecosystems might not easily adjust their mental model to a new, less privacy-respecting smart home ecosystem. While residents can adjust their mental models over time as they interact with or add new devices, visitors might face difficulties in adjusting their mental models as the environment is less well-known to them and might change without their knowledge. Thus, they might rely even more on their – potentially wrong – mental models.

This answers **RQ1**: *What are common privacy perceptions of residents and visitors regarding smart home ecosystems?*

5.2 Misconceptions among Visitors and Residents

Within our study, we identified several misconceptions in the mental models in both roles, but mainly in visitors' mental models.

Visitors often illustrated the data collection in such a way that only devices they actively interact with are able to collect data about them (e.g., the doorbell), while other devices (i.e., those they did not interact with actively) were mostly considered to not collect information about visitors. While this holds true for some devices, it is not representative. Sensors in the environment might indeed collect data about visitors without them interacting actively. However, cameras and motion sensors formed an exception. Similar to smartphones, those devices are more common nowadays and, thus, participants demonstrated better knowledge about them.

Furthermore, visitors underestimated how personal and sensitive collected data about them can be. Visitors frequently thought that registration on the device is necessary such that collected data can be linked to their identity (e.g., login into an account). While this again can be true, the interconnectivity of smart home devices might result in data getting linked to a specific person without previously being registered to an account. This might lead visitors to act in a way that does not match their privacy needs.

Our research confirms this misconception as it has also been demonstrated by related work [42]. While main factors impacting privacy perceptions identified by related work are data sensitivity, familiarity with the environment and trust in the device owner (cf. [19, 41]), we add users' *role* within the smart home ecosystem to this list. Based on our results, we assume that the origin of the misconceptions is not necessarily rooted in technology affinity or understanding, but connected to the users' role within the smart home. In particular, visitors with rather high ATI scores and sophisticated sketches of the smart home ecosystem still showed misconceptions regarding data collected about them. Moreover, participants of both target groups expressed that a connection to the Internet is required for remote control rather than for data collection and processing.

It is particularly alarming that even visitors with advanced mental models about the data flow did not consider data to be linkable to them. That means previous knowledge of a specific smart home device is not enough to judge consequences of data collection. Lastly, (faults in) users' mental models may persist and can highly impact their privacy

perceptions potentially preventing them acting in a way that matches their privacy needs. This addresses **RQ2**: *What are misconceptions of residents and visitors regarding privacy in the smart home ecosystems?*

5.3 Differences in Privacy Perceptions of Visitors and Residents

Our study also provides insights on how the mental models can differ depending on the users' role (resident or visitor). A first main difference is given by different distributions of the mental models considering the level of sophistication. While we did not perform a quantitative analysis, the residents' mental models tended to be more sophisticated. This can result from the active usage of a technology, enhancing the understanding of it.

The second main difference we found in the mental models is based on the perception of devices that collect and store data about residents and visitors. As illustrated above, bystanders underestimated the sensitivity of collected data because they thought the data cannot be linked to their identity. This difference seems to be based on the different perspectives of the investigated roles rather than on their understanding or affinity of technology. While visitors and residents demonstrated a similar level of sophistication in their mental models with detailed knowledge about data collection and storage, visitors in our study missed the connection between the collected data and their identity.

The final main difference is given by the fact that visitors were more likely to demonstrate misconceptions in their mental models than residents. This could prevent them from acting according to their privacy needs.

To summarise, the differences in the mental models are primarily based on the user's role, i.e. resident or visitor. Hence, considering privacy, the user's role is more important then their technology knowledge, answering **RQ3**: *What are differences in the privacy perceptions of residents and visitors regarding smart home ecosystems?*

5.4 Design Challenges & Future Research

With our study, we found that misconceptions depend on roles. Hence, designing privacy mechanisms that specifically target residents, and, more importantly, visitors is crucial. We discuss challenges and directions for future research below.

5.4.1 Increase Awareness & Transparency. Mental models must be sound enough such that users can effectively interact with a technology [34]. Our results show that functional mental models (i.e., those with rather low level of sophistication) are not sound enough to accurately assess data collection and storage in smart homes, which particularly applied to visitors. Additionally, mental models do hardly shift once established [62]. However, increasing transparency of a technology can improve mental models [18].

Means to increase privacy awareness include *privacy labels* for IoT devices' packaging (cf. nutrition labels on groceries) [20, 31, 47]. However, as visitors are usually not involved in the device purchase, this information would not be available for them. Another option is the use of *QR-codes* to provide detailed, privacy-relevant information on IoT devices, to be explicitly accessible for visitors as well [68]. However, to reach and scan the QR-code, visitors potentially need to pass the tracking space of the respective device (e.g., they are already on camera before receiving the respective information). Lastly, *device locators* in the form of LEDs or beep sounds attached to devices can create awareness for their position [58]. While residents might be aware of their own devices' position, this information is particularly relevant for visitors of foreign smart homes (e.g., hotel rooms). However, it is questionable whether the owners of smart home devices would indeed distribute device locators or QR-code stickers in their private homes.

We argue that future mechanisms to increase privacy awareness in smart home environments also need to target visitors. They cannot be assumed to accurately judge implications of data collection and device capabilities, especially if

the visited environment is new to them. Hence, they need assistance. Examples include, but are not limited to, notifying them about data collection on their personal devices (e.g., their smartphone) by a privacy assistance software [15, 36], or visualising spaces of potential tracking by means of augmented reality [54].

Visitors might not have sufficient knowledge about privacy implications of smart homes. Hence, information about IoT devices and respective data collection needs to be made available for visitors, e.g., on their personal devices.

5.4.2 Support Privacy Decisions & Control. Smart home environments provoke a complex interplay between different stakeholders, their social relationship, their attitudes towards privacy, and the smart devices [14]. For instance, visitors and residents might disagree in their preferences towards devices that collect specific data. Two participants in our study even mentioned privacy violations by smart home devices installed by third parties (i.e., the landlord or roommate).

Hence, means to resolve these tensions and negotiate privacy aspects form an integral part of future work. *Visitor modes* have been recommended in related work to mitigate privacy violations [33, 68–70]. Those modes might be a viable solution for smart home environments to adapt to the presence of visitors. Hereby, means for visitors to (automatically) communicate their privacy needs to the smart home environment are crucial. Such mechanisms should prevent visitors from violating the residents' privacy, but at the same time, the opposite should be true. For such a mechanism to be scalable to smart home ecosystems with a plethora of heterogene devices, we argue that it should not even be necessary for visitors to interact with specific devices. Instead, a personal smart device that belongs to them could (automatically or manually) communicate their privacy needs.

Configuring and communicating privacy preferences needs to be possible for visitors without a need to interact with single devices by, e.g., using their personal devices instead. Further, privacy mechanisms for visitors should not interfere with the device owner.

6 CONCLUSION

In this paper, we presented the findings from a qualitative study investigating the privacy mental models of residents and visitors in smart home environments. We interviewed 30 participants (15 in each target group) by means of a drawing exercise and semi-structured interviews. The mental models of our participants had four different levels of sophistication. Those with rather functional mental models miss enough soundness to act following their privacy needs. As further results, we revealed essential differences in the perceptions of visitors and residents regarding the collection and storage of sensitive data. Even though participants in both roles had a similar understanding of the data flow in smart home ecosystems, visitors voiced several misconceptions connected to sensitive data that is captured about them. These misconceptions prevent them from protecting their privacy matching their personal needs. Hence, roles matter more than technology knowledge. Improving the privacy mental models, in particular for visitors who might have limited abilities to act within the environment, constitutes a fundamental challenge due to the heterogeneity of smart home environments and the increasing number of devices. Based on our study, we discuss the limitations of existing solutions and illustrate implications and challenges for the design of future privacy interfaces in smart home environments.

ACKNOWLEDGMENTS

This research was funded by the German Federal Ministry of Education and Research (BMBF) within the SWC 2.0 "PrivacyGate" 01|S17050; 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; by the German Research Foundation (DFG) under grant no. 425869382; and by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr [Voice of Wisdom]. We would further like to thank Andreas Schütz, Stephan Kniep, and Florian Krell who supported the data acquisition of the study.

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 Symposium on Usable Privacy and Security (SOUPS '19)*. 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] Frances K. Aldrich. 2003. *Smart Homes: Past, Present and Future.* Springer London, London, 17–39. https://doi.org/10.1007/1-85233-854-7_2

[5] Florian Alt and Emanuel von Zezschwitz. 2019. Emerging Trends in Usable Security and Privacy. *Journal of Interactive Media (icom)* 18, 3 (Dec. 2019), 1–13. https://doi.org/10.1515/icom-2019-0019

[6] 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

[7] Kang Bing, Liu Fu, Yun Zhuo, and Liang Yanlei. 2011. Design of an Internet of Things-Based Smart Home System. *Proc. ICICIP 2011* 2 (2011), 921–924. https://doi.org/10.1109/ICICIP.2011.6008384

[8] Christine L. Borgman. 1986. The User's Mental Model of an Information Retrieval System: An Experiment on a Prototype Online Catalog. *International Journal of Man-Machine Studies* 24, 1 (1986), 47–64. https://doi.org/10.1016/S0020-7373(86)80039-6

[9] 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

[10] Virginia Braun and Victoria Clarke. 2012. Thematic analysis. (2012).

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

[12] Soumyadeb Chowdhury, Md Sadek Ferdous, and Joemon M. Jose. 2016. Bystander Privacy in Lifelogging. In *Proceedings of the 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

[13] Hyunji Chung, Michaela Iorga, Jeffrey Voas, and Sangjin Lee. 2017. Alexa, Can I Trust You? *Computer* 50, 9 (2017), 100–104. https://doi.org/10.1109/MC.2017.3571053

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

[15] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. 2020. Informing the Design of a Personalized Privacy Assistant for the Internet of Things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376389

[16] 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

[17] 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.

[18] Malin Eiband, Hanna Schneider, Mark Bilandzic, Julian Fazekas-Con, Mareike Haug, and Heinrich Hussmann. 2018. Bringing Transparency Design into Practice. In *Proceedings of the International Conference on Intelligent User Interfaces* (Tokyo, Japan) *(IUI '18)*. Association for Computing Machinery, New York, NY, USA, 211–223. https://doi.org/10.1145/3172944.3172961

[19] 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 Symposium on Usable Privacy and Security (SOUPS '17)*. USENIX Association, Berkeley, CA, USA, 399–412.

[20] 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 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

[21] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human-Computer Interaction* 35, 6 (2019), 456–467. https://doi.org/10.1080/10447318.2018.1456150 arXiv:https://doi.org/10.1080/10447318.2018.1456150

[22] Pranay P. Gaikwad, Jyotsna P. Gabhane, and Snehal S. Golait. 2015. A Survey Based on Smart Homes System Using Internet-of-Things. In *Proceedings of the International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC '15)*. IEEE, Piscataway, NJ, USA, 0330–0335. https://doi.org/10.1109/ICCPEIC.2015.7259486

[23] 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

[24] 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

[25] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. 2013. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future Generation Computer Systems* 29, 7 (2013), 1645 – 1660. https://doi.org/10.1016/j.future.2013.01.010 Including Special sections: Cyber-enabled Distributed Computing for Ubiquitous Cloud and Network Services & Cloud Computing and Scientific Applications — Big Data, Scalable Analytics, and Beyond.

[26] 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 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

[27] Yue Huang, Borke Obada-Obieh, and Konstantin (Kosta) Beznosov. 2020. Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376529

[28] 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 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

[29] Philip N. Johnson-Laird. 1983. *Mental Models: Towards a Cognitive Science of Language, Inference, and Consciousness.* Number 6. Harvard University Press, Cambridge, MA, USA.

[30] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS '15)*. USENIX Association, Berkeley, CA, USA, 39–52.

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

[32] 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 International 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

[33] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. 2021. *"We Just Use What They Give Us": Understanding Passenger User Perspectives in Smart Homes.* Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445598

[34] Todd Kulesza, Simone Stumpf, Margaret Burnett, Sherry Yang, Irwin Kwan, and Weng-Keen Wong. 2013. Too Much, Too Little, or Just Right? Ways Explanations Impact End Users' Mental Models. In *Proceedings of the IEEE Symposium on Visual Languages and Human Centric Computing (VL/HCC '13)*. IEEE, Piscataway, NJ, USA, 3–10. https://doi.org/10.1109/VLHCC.2013.6645235

[35] 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

[36] Marc Langheinrich. 2002. A Privacy Awareness System for Ubiquitous Computing Environments. In *Proceedings of the International Conference on Ubiquitous Computing*. Springer, Cham, Switzerland, 237–245.

[37] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2018. Towards Security and Privacy for Multi-User Augmented Reality: Foundations With End Users. In *Proceedings of the IEEE Symposium on Security and Privacy (SP '18)*. IEEE, Piscataway, NJ, USA, 392–408. https://doi.org/10.1109/SP.2018.00051

[38] 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

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

[40] 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. https://doi.org/10.1016/j.techfore.2018.08.015

[41] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. *"You Just Can't Know about Everything": Privacy Perceptions of Smart Home Visitors.* Association for Computing Machinery, New York, NY, USA, 83–95. https://doi.org/10.1145/3428361.3428464

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

[43] 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

[44] Sarah Mennicken, David Kim, and Elaine May Huang. 2016. Integrating the Smart Home into the Digital Calendar. In *Proceedings of the 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

[45] 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

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

[47] Pardis Emami Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the Experts: What Should Be on an IoT Privacy and Security Label? *ArXiv* abs/2002.04631 (2020), 1–18.

[48] 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 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

[49] Donald A. Norman. 2014. Some Observations on Mental Models. In *Mental Models*. Psychology Press, 15–22.

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

[51] 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. https://doi.org/10.3390/electronics7120379

[52] Sarah Pidcock, Rob Smits, Urs Hengartner, and Ian Goldberg. 2011. Notisense: An Urban Sensing Notification System to Improve Bystander Privacy. In *Proceedings of the International Workshop Sensing Applications on Mobile Phones (PhoneSense '11)*. 1–5.

[53] Sarah Prange and Florian Alt. 2020. I Wish You Were Smart(Er): Investigating Users' Desires and Needs Towards Home Appliances. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '20)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/3334480.3382910

[54] Sarah Prange, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. 2021. PriView– Exploring Visualisations to Support Users' Privacy Awareness. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 69, 18 pages. https://doi.org/10.1145/3411764.3445067

[55] Sarah Prange, Emanuel von Zezschwitz, and Florian Alt. 2019. Vision: Exploring Challenges and Opportunities for Usable Authentication in the Smart Home. In *Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS PW '19)*. IEEE, Piscataway, NJ, USA, 154–158. https://doi.org/10.1109/EuroSPW.2019.00024

[56] 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* (Glasgow, Scotland Uk) *(CHI EA '19)*. ACM, New York, NY, USA, 1–6. https://doi.org/10.1145/3290607.3308458

[57] S. S. I. Samuel. 2016. A Review of Connectivity Challenges in IoT-Smart Home. In *Proceedings of the MEC International Conference on Big Data and Smart City (ICBDSC '16)*. IEEE, Piscataway, NJ, USA, 1–4. https://doi.org/10.1109/ICBDSC.2016.7460395

[58] Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I. Hong. 2020. I'm All Eyes and Ears: Exploring Effective Locators for Privacy Awareness in IoT Scenarios. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376585

[59] Statista. 2019. Smart Home Worldwirde. https://www.statista.com/outlook/279/100/smart-home/worldwide Accessed: January 2021.

[60] Statista. 2020. Smart Home Report 2020. https://de.statista.com/statistik/studie/id/41155/dokument/smart-home-report/ last accessed April 15, 2021.

[61] 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.

[62] Joe Tullio, Anind K. Dey, Jason Chalecki, and James Fogarty. 2007. How It Works: A Field Study of Non-Technical Users Interacting with an Intelligent System. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '07)*. Association for Computing Machinery, New York, NY, USA, 31–40. https://doi.org/10.1145/1240624.1240630

[63] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders Versus Intrusiveness: Teens' and Parents' Perspectives on Home-entryway Surveillance. In *Proceedings of the International Joint Conference on Pervasive and Ubiquitous Computing* (Seattle, Washington) *(UbiComp '14)*. ACM, New York, NY, USA, 129–139. https://doi.org/10.1145/2632048.2632107

[64] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. 2017. Benefits and Risks of Smart Home Technologies. *Energy Policy* 103 (2017), 72–83. https://doi.org/10.1016/j.enpol.2016.12.047

[65] 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

[66] Peter Worthy, Ben Matthews, and Stephen Viller. 2016. Trust Me: Doubts and Concerns Living With the Internet of Things. In *Proceedings of the ACM Conference on Designing Interactive Systems (DIS '16)*. ACM, New York, NY, USA, 427–434. https://doi.org/10.1145/2901790.2901890

[67] 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

[68] 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.

[69] 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 '17)*. USENIX Association, Berkeley, CA, USA, 65–80.

[70] 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 USENIX Security Symposium (USENIX Security '19)*. USENIX Association, Berkeley, CA, USA, 159–176.

[71] 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

[72] 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 (2018), 200. https://doi.org/10.1145/3274469

[73] 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.

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

A CODING TREE

The bullet points represent the categories of our coding tree. The frequency in the two target groups is given in brackets (N_V: visitors, N_R: residents). Data collection and receiving codes follow the structure <IoT device>-<data>.

- **Perceived Control Entities**
  - Central component mentioned (N_V: 9; N_R: 11)
  - Central component not mentioned (N_V: 4; N_R: 4)
  - Central component (if mentioned, multiple codes per participant possible):
    - Server (N_V: 4; N_R: 4)
    - Cloud (N_V: 2; N_R: 1)
    - Smartphone (N_V: 2; N_R: 5)
    - Smart Watch (N_V: 1; N_R: 0)
    - Tablet (N_V: 1; N_R: 1)
    - Generic / unspecified control device (N_V: 2; N_R: 2)
    - Router (N_V: 1; N_R: 3)
    - User (N_V: 0; N_R: 2)
    - local network (N_V: 0; N_R: 1)
    - smart assistant (N_V: 0; N_R: 1)
- **Perceived Data Collection**
  - No interaction with the device
    - camera-video (N_V: 1; N_R: 0)
    - camera-audio (N_V: 1; N_R: 0)
    - smartphone-data (N_V: 3; N_R: 1)
    - smartphone-video (N_V: 1; N_R: 1)
    - smartphone-audio (N_V: 1; N_R: 1)
    - smartphone-location (N_V: 0; N_R: 1)
    - smartwatch-audio (N_V: 2; N_R: 0)
    - smartwatch-data (N_V: 0; N_R: 4)
    - blood pressure sensor-blood pressure (N_V: 0; N_R: 1)
    - mattress-usage (N_V: 0; N_R: 1)
    - lights-usage (N_V: 0; N_R: 2)
    - doorlock-usage (N_V: 0; N_R: 1)
    - tv-audio (N_V: 2; N_R: 0)
    - fridge-audio (N_V: 2; N_R: 1)
    - fridge-temperature (N_V: 0; N_R: 1)
    - jalousie-data (N_V: 0; N_R: 1)

    - window-data (N_V: 0; N_R: 1)
    - smart assistant-audio (N_V: 2; N_R: 3)
    - thermostat-body temperature (N_V: 1; N_R: 0)
    - thermostat-temperature (N_V: 1; N_R: 3)
    - surveillance system-video (N_V: 2; N_R: 3)
    - smoke detector-status (N_V: 0; N_R: 2)
    - vacuum cleaner-data (N_V: 0; N_R: 2)
    - plug-usage (N_V: 0; N_R: 1)
  - By interaction with the device
    - mattress-data (N_V: 2; N_R: 0)
    - fridge-video (N_V: 2; N_R: 1)
    - fridge-order (N_V: 0; N_R: 1)
    - doorlock-data (N_V: 2; N_R: 1)
    - doorbell-video (N_V: 3; N_R: 1)
    - tv-data (N_V: 5; N_R: 0)
    - smart assistant-audio (N_V: 3; N_R: 3)
    - smartphone-data (N_V: 0; N_R: 3)
    - smartwatch-data (N_V: 5; N_R: 1)
    - vacuum cleaner (N_V: 1; N_R: 0)
    - light-usage (N_V: 3; N_R: 0)
    - plug-data (N_V: 1; N_R: 0)
    - brush-usage (N_V: 0; N_R: 2)
  - Via interaction with other devices
    - light-motion (N_V: 1; N_R: 0)
    - smart meter-energy consumption (N_V: 1; N_R: 0)
- **Perceived Data Receiving**
  - No interaction with the device
    - camera-video (N_V: 1; N_R: 0)
    - camera-audio (N_V: 1; N_R: 0)
    - smartphone-video (N_V: 2; N_R: 0)
    - smartphone-audio (N_V: 2; N_R: 1)
    - smartphone-messages (N_V: 0; N_R: 1)
    - smartwatch-audio (N_V: 1; N_R: 0)
    - smartwatch-messages (N_V: 0; N_R: 1)
    - smartwatch-data (N_V: 0; N_R: 1)
    - fridge-data (N_V: 0; N_R: 1)
    - heater-body temperature (N_V: 1; N_R: 0)
    - heater-temperature (N_V: 0; N_R: 1)
    - smart assistant-audio (N_V: 2; N_R: 0)
    - surveillance system-video (N_V: 3; N_R: 1)
    - thermostat-body temperature (N_V: 1; N_R: 0)
    - vacuum cleaner-data (N_V: 0; N_R: 3)
  - By interaction with the device
    - vacuum cleaner-data (N_V: 1; N_R: 1)
    - smartphone-data (N_V: 0; N_R: 1)
    - smartwatch-audio (N_V: 6; N_R: 0)
    - smartwatch-location (N_V: 0; N_R: 1)
    - mattress-body data (N_V: 2; N_R: 0)
    - fridge-video (N_V: 2; N_R: 0)
    - doorbell-video (N_V: 4; N_R: 0)
    - tv-data (N_V: 3; N_R: 0)
    - smart assistant-audio (N_V: 3; N_R: 2)
    - light-usage (N_V: 2; N_R: 4)
    - thermostat-usage (N_V: 1; N_R: 0)
    - doorbell-video (N_V: 1; N_R: 0)
    - plug-data (N_V: 1; N_R: 0)
    - smoke detector-smoke (N_V: 1; N_R: 0)
    - jalousie-data (N_V: 0; N_R: 1)
    - window-data (N_V: 0; N_R: 1)
  - Via interaction with other devices
    - light-motion (N_V: 1; N_R: 0)
    - smart meter-energy consumption (N_V: 1; N_R: 0)
- **Perceived Storage Location**

- Local server / Internal Storage (N_V: 4; N_R:4)
- (External) Cloud (N_V: 3; N_R: 3)
- Internet / Server (N_V: 0; N_R: 3)
- IoT Devices (N_V: 5; N_R: 0)
- Smartphone (N_V: 1; N_R: 1)
- Provider (N_V: 8; N_R: 7)
- Apps (N_V: 2; N_R: 0)
- User (N_V: 1; N_R: 0)
- Hackers (N_V: 1; N_R: 0)
- Marketing Companies (N_V:0; N_R: 1)
- No idea (N_V: 1; N_R: 0)
- Not mentioned (N_V: 0; N_R: 3)

B IUIPC

Detailed values for all 10 IUIPC items [38] and all participants of both target groups, residents and visitors.

Table 3. Participants' IUIPC ratings (10-item version [38]), for residents and visitors.

		Residents		Visitors	
		Mean	SD	Mean	SD
Control	Consumer online privacy is the consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.	6.33	0.72	6.00	1.20
	Consumer control of personal information lies at the heart of consumer privacy.	6.33	0.62	5.93	1.16
	I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.	5.8	1.32	6.06	1.10
Awareness	Companies seeking information online should disclose the way the data are collected, processed, and used.	6.07	1.28	6.13	1.19
	A good consumer online privacy policy should have a clear and conspicuous disclosure.	6.46	1.06	6.13	1.06
	It is very important to me that I am aware and knowledgeable about how my personal information will be used.	6.07	1.16	5.73	1.53
Collection	It usually bothers me when online companies ask me for personal information.	4.87	1.4	5.40	1.40
	When online companies ask me for personal information, I sometimes think twice before providing it.	5.8	1.08	5.33	1.45
	It bothers me to give personal information to so many online companies.	5.47	1.19	5.60	1.45
	I'm concerned that online companies are collecting too much personal information about me.	5.53	1.55	5.00	1.60

C DEVICES FOR DRAWING EXERCISE

Table 4 on the next page shows the categories and respective devices that we provided for the drawing exercise. Each participant was asked to choose (at least) one of each category to ensure that they consider a whole smart home ecosystem. The participants were allowed to add further entities if they wished so. The table also shows how many participants of each target group (residents, visitors) in our study choose the respective device to explain their understanding of the data flow in a smart home ecosystem.

Table 4. Overview of Devices: Participants chose one device per category for their mental model drawing.

		Residents	Visitors	Sum
Entertainment Communication	smartphone	8	7	15
	smart assistant	5	3	8
	smart hub	1	0	1
	smart speaker	0	0	0
	smart TV	1	5	6
Energy Management	smart lights	8	7	15
	smart heating	4	3	7
	smart plugs	3	4	7
	smart water meter	0	1	1
	smart electricity meter	0	0	0
Security Safety	smart smoke detector	5	5	10
	smart surveillance	4	3	7
	smart doorbell	2	4	6
	smart lock	2	3	5
	smart window sensor	2	0	2
Health	smart watch	8	12	20
	smart brush	4	1	5
	smart matress	0	2	2
	smart blood pressure	1	0	1
	smart sleep sensor	2	0	2
Home Automation	smart vacuum	6	2	8
	smart jalousie	3	4	7
	smart fridge	3	4	7
	smart thermostat	3	3	6
	smart coffee machine	0	2	2

D MENTAL MODELS OF THE SMART HOME ECOSYSTEM PER PARTICIPANT

Table 5. Distribution of mental models about the smart home ecosystem, ATI scale and IUIPC scales among participants of both target groups, including their employment status and living situation.

ID	Target Group	employment status	living situation	Mental Model	ATI	IUIPC Scales Control	Awareness	Collection
PU1	Resident	student	with partner	advanced understanding	5.78	6.33	6.33	4.25
PU2	Resident	student	family	basic understanding	3.67	4.66	3.33	5.50
PU3	Resident	student	with partner	advanced understanding	3.56	6.33	5.33	4.00
PU4	Resident	student	family	basic understanding	4.00	6.66	6.33	5.75
PU5	Resident	student	family	advanced understanding	3.44	6.66	6.33	5.5
PU6	Resident	other	in a flat share	advanced understanding	4.56	6.00	7.00	3.50
PU7	Resident	student	in a flat share	high-level understanding	5.11	5.66	6.00	4.75
PU8	Resident	self-employed	alone	basic understanding	2.00	6.66	6.66	6.00
PU9	Resident	self-employed	alone	basic understanding	2.89	5.66	6.33	5.75
PU10	Resident	student	family	high-level understanding	5.00	6.66	6.66	5.50
PU11	Resident	self-employed	with partner	high-level understanding	4.67	6.33	7.00	5.50
PU12	Resident	employed/self-employed	with partner	high-level understanding	4.67	6.66	5.66	4.75
PU13	Resident	student	in a flat share	schematic simplification	2.56	6.66	7.00	7.00
PU14	Resident	employed	alone	advanced understanding	4.33	6.66	7.00	6.75
PU15	Resident	self-employed	family	schematic simplification	4.67	4.66	6.00	6.75
PB1	Visitor	employed full time	with partner	advanced understanding	4.78	6.00	5.66	5.25
PB2	Visitor	employed full time	alone	advanced understanding	4.11	6.00	7.00	6.25
PB3	Visitor	student	with partner	advanced understanding	4.67	5.33	4.66	4.25
PB4	Visitor	student	with partner	schematic simplification	2.78	6.33	6.33	6.00
PB5	Visitor	student	in a flat share	advanced understanding	3.56	6.00	3.66	4.50
PB6	Visitor	student	with partner	basic understanding	4.56	5.00	4.66	2.50
PB7	Visitor	student	family	advanced understanding	5.56	7.00	6.33	6.50
PB8	Visitor	student	family	schematic simplification	4.33	5.00	6.00	5.75
PB9	Visitor	student	family	basic understanding	5.00	7.00	7.00	6.25
PB10	Visitor	employed full time	with partner	high-level understanding	4.22	7.00	7.00	6.75
PB11	Visitor	student	alone	schematic simplification	4.33	7.00	7.00	6.25
PB12	Visitor	student	family	schematic simplification	3.67	4.00	6.00	3.50
PB13	Visitor	student	family	schematic simplification	4.56	5.33	6.66	4.00
PB14	Visitor	other	alone	basic understanding	4.11	7.00	5.00	6.50
PB15	Visitor	student	in a flat share	advanced understanding	4.67	6.00	7.00	5.75