Privacy Perceptions and Designs of Bystanders in Smart Homes

YAXING YAO, School of Information Studies, Syracuse University, USA
JUSTIN REED BASDEO, School of Design, Syracuse University, USA
ORIANA ROSATA MCDONOUGH, School of Information Studies, Syracuse University, USA
YANG WANG, School of Information Studies, Syracuse University, USA

As the Internet of Things (IoT) devices make their ways into people's homes, traditional dwellings are turning into smart homes. While prior empirical studies have examined people's privacy concerns of smart homes and their desired ways of mitigating these concerns, the focus was primarily on the end users or device owners. Our research investigated the privacy perceptions and design ideas of smart home bystanders, i.e., people who are not the owners nor the primary users of smart home devices but can potentially be involved in the device usage, such as other family members or guests. We conducted focus groups and co-design activities with eighteen participants. We identified three impacting factors of bystanders' privacy perceptions (e.g., perceived norms) and a number of design factors to mitigate their privacy concerns (e.g., asking for device control). We highlighted bystanders' needs for privacy and controls, as well as the tension of privacy expectations between the owners/users and the bystanders in smart homes. We discussed how future designs can better support and balance the privacy needs of different stakeholders in smart homes.

CCS Concepts: • **Security and privacy → Human and societal aspects of security and privacy**; Social aspects of security and privacy;

Additional Key Words and Phrases: Smart home; bystanders; collaborative privacy; co-design

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

1 INTRODUCTION

Various Internet of Things (IoT) devices have made their way into people's homes, turning traditional dwellings into *smart homes*. These devices infiltrate households and aim to provide efficiency and usability for homeowners. At the same time, the Internet-connected nature and the amount of data collected by these IoT devices pose great privacy risks to users. A 2015 report by the Federal Trade Commission has shown that fewer than 10,000 households with smart home IoT devices can generate 150 million discrete data points per day [10]. This massive amount of data allows a variety of analyses which are not possible using other data [10].

Authors' addresses: Yaxing Yao, School of Information Studies, Syracuse University, Syracuse, NY, 13244, USA, yyao08@syr.edu; Justin Reed Basdeo, School of Design, Syracuse University, Syracuse, NY, 13244, USA, jrbasdeo@syr.edu; Oriana Rosata Mcdonough, School of Information Studies, Syracuse University, Syracuse, NY, 13244, USA, ormcdono@syr.edu; Yang Wang, School of Information Studies, Syracuse University, Syracuse, NY, 13244, USA, ywang@syr.edu.

2573-0142/2019/11-ART59 $15.00
https://doi.org/10.1145/3359161

From the perspective of smart home users, many prior studies have investigated users' privacy perceptions of smart homes and have discovered a number of privacy concerns, such as sensitive data collection [48], data sharing [47], and data misuse and re-purpose [26]. However, little is known about other stakeholders' privacy perceptions in smart homes, such as visitors, tenants, other family members, etc. This is an important aspect to consider in the development of smart homes because these other stakeholders' privacy is often ignored and can even be violated without their knowledge. For example, a recent news article reported that smart home devices that can record people's voice often pick up other people (e.g., spouse, friends, kids) talking in the background [36]. In the real world, such cases often happen in scenarios where guests visit other people's homes and are exposed to other people's smart home devices. This case demonstrates that the privacy risks for other people in smart homes indeed exist, however, their understanding and privacy perceptions are understudied in the prior literature. In addition, people may face other situations that can potentially invade their privacy, e.g., an Airbnb host may have access to security camera data while the tenant may not due to the power imbalance between the owner and the tenant [14].

This paper focuses on one specific group of stakeholders in smart homes, i.e., bystanders. In this paper, we use smart home **owners/users** to denote people who directly purchase smart home devices. In other words, owners/users in our study context refer to people who *own* smart home devices. We use smart home **bystanders** to refer to people who do not own or directly use these devices but are potentially involved in the use of smart home devices, such as other family members who do not purchase the devices, guests, tenants, passersby, etc.

Our study attempts to fill the gap in the literature by specifically investigating smart home bystanders' privacy perceptions. In particular, through a focus group study with eighteen bystanders in six groups, we aimed to understand the concerns that bystanders had towards smart homes under a variety of social contexts. In the last part of the focus group, we adopted a co-design approach [33–35] and collaborated with bystanders to design privacy mechanisms to mitigate their privacy concerns in smart homes.

This paper makes three contributions. First, we investigate smart home bystanders' privacy concerns and identify several factors that affected their privacy perceptions, such as trust towards the owners. Second, the design activity results in a number of design factors that bystanders considered when designing privacy mechanisms to protect their privacy. These perceptions and the design factors demonstrate bystanders' needs for privacy and some control mechanisms. We highlight the cooperative design mechanism as a unique aspect of bystanders' privacy designs and advocate for addressing privacy needs for both owners/users and bystanders through potential collaboration. Third, we make a number of concrete design suggestions to better support different stakeholders' privacy needs in smart homes.

2 RELATED WORK

In this section, we present the prior literature on privacy issues in smart homes in general and different privacy mechanisms. We then summarize prior research on understanding the bystanders' perspective in introduce the bystanders' perspective in prior research and explain why our results fill a significant gap in the literature.

2.1 Smart Home Privacy Risks and Concerns

Given improvements in smart home technologies, researchers have started to look at the potential privacy and security risks associated with changes in technology. These risks include but are not limited to: the possibility of identity theft and device reconfiguration [4], the inference of user activities at home through smart home network traffic analyses [2], as well as risks caused by human factors (e.g., weak passwords) and system flaws (e.g., unauthorized system modifications) [21].

User studies also looked at the privacy issues of smart homes from the perspective of end-users. From the smart home level, people were concerned about the possibility of Internet attacks and data abuse [49]. Zeng et al.'s interview study discovered people's concerns on video recording, data collection, and analysis, as well as network hacking [47]. However, their participants also outweigh cost and interoperability over privacy and security [47]. Worthy et al. found an association between people's trust towards the entities that collected their information and their desired control of such information, and they argued that less trust would lead to a greater level of desired control [40]. Brush et al. further claimed that a "difficulty achieving security" was one road blocker towards large adoption of smart home devices. On the other hand, according to Zheng et al., some people believed that their privacy was well protected by the entities who collected the information, which may result in new privacy risks [48]. In a slightly different direction, Apthorpe et al.'s survey study investigated the privacy norms in smart homes using the theory of Contextual Integrity and found a number of factors that could influence specific norms, such as their purposes of device usage (e.g., in an emergency situation) and device ownership (e.g., how many devices users owned) [3]. To explore what information should be provided to the users in smart homes, Jakobi et al. conducted a long term study and identified users' information demands to understand smart home system performance and communications [22]. They found that in the initial phase of smart home usage, users preferred to access detailed information of the smart home environment through web-based platforms, whereas in the later stage, users preferred to only know the exceptions where something went wrong [22]. In a recent work, Barbosa et al. discovered that factors such as "consent not given" and "sensitive data collection" could make users less comfortable, and factors such as "user control" and "user awareness" could make users more comfortable regarding the data collection in a smart home [29].

Concerning especially about smart home devices, users have shown their uncertainty of data practices in smart TVs, including data collection, usage, re-purposing, and sharing with third-parties [26]. For smart toys, parents were concerned about data collection and sharing abilities while children were uncertain of whether their conversations with the toys could be heard by their parents [27]. Interestingly, smart speaker users generally expressed no concerns in their perceptions, but the rationale behind their perceptions (e.g., they did not mention any concern because they had strong trust towards device manufacturers) could lead to more serious privacy risks [24]. In fact, when users did not have concerns toward smart home devices, it did not mean that the users do not face any privacy risks. For example, users' activities can be inferred using their smart home network data and thus pose various privacy risks to the users [1].

2.2 Bystanders' Privacy Concerns

The privacy of bystanders has been studied in a few contexts. For example, Denning et al. found that bystanders assumed augmented reality wearable devices were used for recording [13]. In their study, they reported cases in which bystanders had negative reactions to these devices and expected to be asked for consent before they were captured by them [13]. Bystanders' privacy was a concern of people who recorded audio or video for lifelogging [20]. As such, the recorder chose to discard, modify, or not share the audios or videos to respect the privacy of bystanders [19]. Wang et al. studied bystanders' privacy perceptions of drones in a variety of usage scenarios and discovered several privacy concerns held by bystanders, such as peeking and stalking, as well as surveillance in public places [38]. Interestingly, when comparing drone bystanders' privacy perceptions with the drone controllers', Yao et al. identified several mismatches. For example, bystanders were heavily concerned about their faces being recognized in drone footage while controllers believed that drone cameras were satisfactory for such purposes [44]. Motivated by this line of research, in our paper, we investigate the privacy perceptions of bystanders in the context of smart homes. Besides, we

aim to identify, if any, mismatches in the perceptions between users/owners and bystanders to further inform future privacy designs.

2.3 Smart Home Privacy Mechanisms

Many technical solutions have been proposed to mitigate smart home privacy risks and concerns. To reduce the potential of inferences, Yoshigoe et al. designed a software-based system to automatically inject synthetic network packets to obscure legitimate network data flow [46]. Apthorpe et al. demonstrated the effectiveness of introducing noise data to shape smart home network traffic [2] to obscure the real traffic and prevent data loss. A more recent work by Datta et al. introduced a Python library so that developers could easily implement traffic shaping for IoT devices [12]. To achieve better access control to users' data, Moncrieff et al. designed a tool to manage access privileges dynamically and automatically according to some contextual factors in home surveillance, such as users' activity and location in the home [28]. Through capturing user-defined privacy zones and generating corresponding policies dynamically, Arbo et al.'s framework aimed to ensure data security for smart home devices [4]. Chakravorty et al.'s system only granted users access to their data if these users were successfully re-identified by the system [8]. To increase data transparency and user awareness as well as to facilitate user control, Das et al. envisioned an infrastructure to personalize users' privacy notices based on their privacy preferences in IoT devices [11]. Wang et al. built a tool which could blur faces captured by cameras based on users' self-defined rules [37]. McReynolds et al. suggested that smart toys should communicate their recording capabilities to the parents and children [27]. Lastly, Lin et al. suggested a mechanism in which supporting systems should auto-configure new devices added to the smart home network based on the most secure setting to ensure a safe home environment [25].

Arguing that the above privacy mechanisms were proposed or implemented either by researchers or experts without users' input, Yao et al. took a user-centered approach in which they involved smart home users and co-designed privacy-enhancing mechanisms to alleviate users' privacy concerns [42]. Their study suggested several factors and features that users considered in their designs, such as network intrusion detection and data localization [42].

2.4 Gap in the Literature

We aim to explore how **bystanders perceive privacy issues in smart homes**. This is an important question for two reasons. First, bystanders' privacy issues are usually omitted. This is because bystanders are not the owners nor users of smart homes, however, they are subject to usage of smart home devices without their knowledge for most of the time. Understanding bystanders' privacy perceptions can broaden our knowledge of smart home privacy issues more holistically. Second, the rapidly growing popularity of smart home devices has created many interesting yet controversial social contexts in which users receive benefits from these devices but may put bystanders' privacy at risk (e.g., using an Internet-connected security camera in an Airbnb apartment [17] and the adoption of voice assistants in hotel rooms [9]). Understanding the factors that influence bystanders' privacy perceptions of smart homes can provide insights into how to better suit the needs of both users and bystanders collaboratively.

In addition, inspired by Yao et al. [42], we deem to see what privacy mechanisms bystanders desire to mitigate their privacy concerns if exist. The results can inform future privacy designs and illuminate how to support the privacy needs of both bystanders and users. Next, we will describe our methodology in detail.

Table 1. Summary of participants' demographics

Group	Participants	Gender	Age	Occupation	Experiences	Scenarios
1	P1	M	18-25	Student	Owner	S1, S2
	P2	F	18-25	Student	Owner	S1, S2
	P3	M	18-25	Student	Owner	S1, S2
2	P4	M	36-45	Hospital employee	Owner	S1, S2
	P5	M	26-35	Government employee	Owner	S1, S2
	P6	F	26-35	Student	Experienced	S1, S2
3	P7	F	18-25	Paralegal	Owner	S2, S3
	P8	M	26-35	University staff	Owner	S2, S3
	P9	F	36-45	Postal expeditor	Experienced	S2, S3
	P10	M	36-45	Civil engineer	Owner	S2, S3
4	P11	M	>65	Retired	Non-user	S1, S3
	P12	F	26-35	Unemployed	Experienced	S1, S3
5	P13	F	36-45	Sales	Experienced	S1, S3
	P14	M	56-65	Retired	Non-user	S1, S3
	P15	F	>65	Retired	Non-user	S1, S3
6	P16	M	26-35	Editor	Owner	S2, S3
	P17	F	26-35	Filmmaker	Owner	S2, S3
	P18	F	36-45	Chef	Experienced	S2, S3

3 METHOD

To explore bystanders' privacy expectations and how they desire to protect their privacy, we conducted six focus groups with an average of three participants in each group and a total of eighteen participants. We chose to do focus groups instead of one-on-one interviews because we hoped to encourage interaction between participants and spark the discussion by bringing different experiences as bystanders. The average length of the sessions was 1.5 hours. Upon completion, each participant was paid $15. This study is approved by our university IRB.

3.1 Study Settings

Participants recruitment. We recruited our participants primarily through Craiglist, word-of-mouth, and local senior citizen centers. When prospective participants first reached out to us, we asked them to fill a pre-screening survey to obtain their demographic information. We deliberately selected participants from various gender identities, age groups, occupations, and with different levels of smart home experiences. We carefully framed our study as "a focus group study to understand your perceptions of smart homes" without mentioning anything related to "privacy" to prevent potential bias. We summarize the demographics of the participants and their groups in Table 1.

Pilot study. Drawing from prior research [13, 19, 33–35, 38, 42, 45], we developed a list of questions and activities to probe participants to think about the potential benefits and concerns of smart homes from the perspective of bystanders. We ran two pilot study sessions with seven participants, gained a few insights, and then made several changes to our study protocol. First, in the initial protocol, we only asked participants to think from the bystanders' perspective. In the

pilot study, we found that our participants tended to think from the owners' perspective. Thus, we added a question and asked the participants to recall the last time they visited other people's places where smart home devices were installed to better situate them as bystanders. Second, the original protocol asked participants about their general perceptions and concerns of smart home devices. However, in the pilot study, we found that our participants focused more on the negatives of smart homes in the scenarios. Thus, to reduce potential priming, we asked participants to discuss the benefits first in each scenario to ensure they think thoroughly. Third, when we asked our participants to create prototypes to illustrate their ideas, most of them expressed confusions on the definition of "prototypes". Thus, we added a brief introduction session to show participants a few examples of different types of prototypes (e.g., diagram, low-fidelity paper prototypes, wireframe, etc.) to help them know the expectations from the design activity. The final study protocol is described in detail in the next section.

3.2 Study Flow

The goal of the study is to understand bystanders' privacy expectations in smart homes and their desired privacy controls. We divide each study session into three main parts.

Part 1: general understandings. We started each session with a round-table introduction. We first asked each participant to talk about their understandings, experiences, and general perceptions regarding smart home technologies. Regardless of their prior knowledge, we provided a working definition of smart home [7, 23], *"a home consists of different sensors, systems, and devices, which can be remotely controlled, accessed, and monitored."* We showed them a few smart home devices and explained their primary functions. These devices included voice assistants, security cameras, smart toys, and a set of smart appliances.

Before introducing the concept of "bystanders", we first asked participants to discuss the pros and cons of smart homes in general. We then started to shift the perspective towards that of bystanders by asking participants to describe their past experiences and thoughts in other people's smart homes. Next, we deliberately introduced our definition of a "bystander" in the smart home context, framing it as *"people who are not the owners nor the primary users of smart home devices but can potentially be involved in the device usage."* We then asked our participants to think about themselves as the bystanders in the remainder of the study.

Part 2: scenario-based discussions. Similar to [39, 43], we introduced three scenarios in our study to (1) capture participants' contextual privacy perceptions and (2) better situate our participants and nudge them to think as bystanders. The three scenarios were inspired either by findings in the literature or from the news, including: (1) *the temporary residency scenario (S1):* you rented an apartment for three days through Airbnb and an Internet-connected security camera was installed in the apartment [17]; (2) *the playdate scenario (S2):* you took your child to a playdate and there was a smart toy for the kids to play with [16]; and (3) *the cohabitant scenario (S3):* you live in your own house and your spouse purchased an Amazon Echo [48]. These scenarios were designed to represent a variety of factors, including different application contexts (e.g., temporary resident in an Airbnb apartment, friend's house, your own house), social relationships (e.g., tenants and owners, guests and owners, husband and wife), and different devices (e.g, Internet-connected security cameras, voice assistants, smart toys). It is worth noting that we did not limit our participants to these devices. All participants were told that they could also discuss other devices they would like to add in each scenario. We also did not explicitly mention or investigate the case of hidden devices (e.g., devices that were purposefully hiding in a place by the owners or not obvious to the bystanders) because we did not want to prime our participants to think about devices that were not obvious to them which could adversely influence their perceptions. Due to time limitations, each

group was asked to discuss two of the three scenarios. For each scenario, we asked our participants to discuss the benefits of smart homes as bystanders, then we moved forward to discuss their concerns.

When finishing the discussion of the scenarios, our participants demonstrated to have grasped the concept and the role of bystanders for the study. These prior activities resulted in participants' understandings of a wide range of potential benefits as well as potential concerns, including their privacy concerns and expectations. We then focused on the privacy concerns and expectations emerged from the discussion and continued the study with a co-design activity.

Part 3: co-design of privacy mechanisms. The goal of this activity was to co-design privacy-enhancing mechanisms with our participants based on their privacy concerns and expectations in smart homes as bystanders. We first situated participants in a friend's house with a number of smart home devices (i.e., voice assistants, security cameras, and smart toys, all adopted from the previous three scenarios) presented, then we asked them to brainstorm their desired features to mitigate their aforementioned privacy concerns and created prototypes to illustrate their ideas. We chose to use a different and more general scenario with the same devices for the design activity rather than using the three scenarios from the previous part for two considerations. First, each group of participants only discussed two of the three scenarios, thus none of the three scenarios were shared by all three groups. Besides, involving all participants in the same scenario made it easier to synthesize our findings. All previous scenarios were designed with different combinations of contextual factors in mind which made it difficult to understand the rationale behind participants' designs. We provided a set of tools (e.g., Post-It notes, color pens, paper board, color papers) for their convenience. We encouraged participants to collaborate and discuss their ideas with others and with researchers, break the existing technological and policy limitations, and potentially design futuristic and speculative solutions.

3.3 Data Analysis

Study recordings. All study sessions were audio-recorded after obtaining participants' consent. Then two co-authors transcribed all recordings and conducted a thematic analysis [6]. We read all transcriptions a few times to familiarize ourselves with the data, then coded one transcription (i.e., the transcription of one complete focus group) together at the sentence level. After generating the initial codebook, we independently coded the same subset of data. When new codes emerged from this process, we added them to the codebook. Upon completion, we compared and discussed the coding and merged their codebook. The inter-coder agreement was 0.81 (Cohen's Kappa), which is considered good [15]. Then we coded the rest of the data using the updated codebook. The final codebook contained over 120 unique codes, such as "bystander action", "trust in the owner", and "wish for data local storage". We further grouped all codes into seven themes, including "general perceptions", "perceived norms", "bystanders' awareness", "privacy-seeking behaviors", "cooperative mechanisms", "bystander-centric mechanisms", and "demographics". We deliberately checked all the codes to ensure they were assigned to the appropriate groups.

Image data. We collected participants' prototypes of their designs. Using the same analysis method in Poole et al.'s study [32], two co-authors coded all the elements in the prototypes. These elements covered everything that was covered in the prototypes, including all components (e.g., stakeholders, devices), visual elements (e.g., buttons, colors), information flow (e.g., information type, flow directions), and other parts (e.g., notes). We followed the same coding procedure as described above and resulted in a codebook with over 100 codes. We further grouped all codes into six themes. The inter-coder agreement was 0.85 (Cohen's Kappa), which is considered good [15].

4 RESULTS

Next, based on our thematic analysis, we first focus on the themes related to our participants' privacy perceptions, then we present the main themes from our participants' privacy designs.

4.1 Participants' General Perceptions

Our participants discussed several benefits of adopting smart home technologies, including enabling home automation, providing remote access, ensuring home safety, etc. They acknowledged several benefits of using smart home devices in all scenarios. We summarize the perceived benefits in this section. The full list of the perceived benefits and risks discussed by our participants is attached in Table 3 in the Appendix. For example, in the temporary residence scenario, bystanders mentioned that if the apartment was a shared space, having some smart home devices (e.g., an Internet-connected security camera) could provide them a peace of mind for safety purposes. Our participants' concerns of smart home devices varied among individuals and across different scenarios. In general, bystanders' had more privacy concerns in the temporary residence scenario and the playdate scenario than the cohabitant scenario. Bystanders also expressed more concerns regarding the video and audio data collected by devices with microphones and cameras (e.g., voice assistants, security cameras) but barely any concern with other devices (e.g., smart coffee makers).

Through our analysis, we identified three major aspects to shape bystanders' privacy perceptions of smart home devices: their perceived norms in different contexts, their awareness of smart home devices and device behaviors, and the potential ways to control their privacy. In the following section, we unpack the three aspects and describe how each aspect shapes bystanders' privacy perceptions.

4.2 Three Aspects of Bystanders' Perceptions

4.2.1 Perceived Norms. Perceived norms refer to bystanders' believed values or standards in a given context. For example, our participants felt that as bystanders, they should not directly control the devices without the owners' permission. Such norms are deeply rooted into specific contexts and contain four primary facets: (1) perceived device utility, (2) perceived social relationship, (3) perceived trust, and (4) length of stay. Changes to any one of the facets may cause changes to bystanders' perceived norms, which further influence their privacy perceptions. We present the four facets below.

Perceived device utility. The first facet of the perceived norms is bystanders' perceived device utility. This facet was brought up by eight participants (P1-3, P5-6, P8, P14, P17). Bystanders held different opinions on whether smart home devices were needed in this context. For instance, in the temporary residency scenario, several bystanders believed the legitimacy of having Internet-connected security cameras installed in the apartment for security reasons (e.g., if the shared space was broke in or needed surveillance) as long as the cameras were not in the bedroom or living room. However, some other bystanders were completely against the use of cameras inside an Airbnb apartment since they preferred to have their privacy. In the playdate scenario, P6 shared her opinion about smart toys:

"My concern would just be that the kid grows up used to having invasive devices present so I would prefer the Alexa not in the house and the toy not in the house ... because I would imagine the purpose of the toy is to get children used to having smart devices and other smart amenities. Personally, I would want my child to be more concerned about their privacy." (P6)

P6's perceived utility of smart toys significantly affected her perceptions. She believed that this device was designed to immerse the children in an environment full of "smart amenities" so that they would get used to these devices, instead of being an object that the children could simply play

with. In the long run, children would be used to the data collection and potential privacy violations associated with such devices. Thus, she would be concerned.

Social relationship. The social relationship in the study mainly refers to bystanders' relationships with the owners of smart home devices. Such a relationship also helps to shape bystanders' perceptions. This facet was discussed by seven participants (P1, P3, P5-7, P10, P14). For example, P10 commented on how social relationships impacted his perception:

"Listening to children doesn't make sense to me. I would like that kid playing with another toy. If it is my friend's kid and they assure me that the toy is fine, I would be ok. If I'm not close with the other parent, I would try to politely get my kid not to play with it. " (P10)

P10 believed that smart toys needed to listen to and record children's conversation to provide the "smart features." His privacy perception of the smart toys from a bystander's perspective largely depended on the relationship between himself and the owners. In this case, he would allow his children to play with the smart toy if the owner was a close friend. In the cohabitant scenario, P16 was against the use of any smart home devices due to the potential collection of his data. However, he also acknowledged that he would still use the voice assistant if his wife bought it and wanted to use it, which further confirmed the role of social relationships in influencing bystanders' perceptions.

Perceived trust. Perceived trust refers to bystanders' perceived trust level towards different potential stakeholders involved in smart homes, such as the owner, the device manufacturers, as well as the potential mediators (e.g., Airbnb as the company in the temporary residency scenario). This was discussed by seven participants (P1, P3, P6-7, P10-12). For example, in the temporary residency scenario, bystanders discussed their trust towards the owner of the property. P12 refused to book an apartment even if she was told explicitly that there was a security camera in the home. She explained:

"I like my privacy. You can say there's ownership and it's their building, but I guess I don't trust people, expect the worst of people I guess. I wouldn't like that." (P12)

P12's lack of trust towards the apartment owner was the primary reason for not accepting the usage of a security camera. Besides, bystanders also mentioned how their trust towards the manufacturers and the mediators influenced their privacy perceptions (e.g., they tend to trust the household company names and believe in their privacy policy), further confirming the findings from prior research [24, 47].

Length of stay. Length of stay is a unique facet in smart home norms from bystanders' perspectives. It refers to how long a bystander stays at one particular location.This was discussed by three participants (P2, P4, P15). Our results suggested that the length of stay also impacted bystanders' privacy perceptions. Generally, bystanders were more concerned with smart home devices if they were exposed for a longer time, although different participants had different interpretations towards what a "long time" meant. For example, P2 believed that in the temporary residency scenario, "three days" could be considered as a long time, thus using an Internet-connected security camera and other smart home devices was not acceptable. However, P4 had a different opinion on this and explained:

"I think this would be different if this was at a friend's house or I was renting an apartment and the apartment owner was like we have to have cameras on you at all times because this is a short amount of time. If this was a long time, like three weeks, or if it was someone I don't trust and there were no laws against it, then that is a red flag." (P4)

In this response, P4 not only explained his perceived "a long time" being three weeks but also further echoed the aforementioned trust facet. His privacy perceptions as a bystander would vary if these two facets changed. P4's quote also hinted that regulations would play a role in his perceptions.

However, we did not observe recurring theme around users' legal expectations. Future research may dive deep into this area.

The above examples further suggested that, due to the complex social dynamics in smart homes, the social norms were not always clear, which made privacy management more difficult in smart homes when considering both bystanders and owners. We will further unpack the implication in the Discussion section.

4.2.2 Bystanders' Awareness of the Smart Homes. The second aspect influencing bystanders' perceptions is related to their awareness of the surrounding environment. Such awareness further includes their awareness of smart home devices one owners' property and their knowledge of smart home device behaviors.

Awareness of device existence. This was discussed by thirteen participants (P1-4, P6-8, P10, P11-P13, P16, P17). Many bystanders acknowledged that often times, they did not pay attention to or look for any smart home devices even though those devices were becoming more and more ubiquitous. It is worth noting that although we did not explicitly investigate the issue of hidden devices, the awareness issue still emerged from our study as one main factor that impacted bystanders' perceptions. Our participants discussed their thoughts about the consequences of not knowing the existence of these devices. As P8 stated, controlling the devices was not as big an issue since he could negotiate with the owners. However, unawareness of the devices was a vastly different story. One thing worth noting from our study was the fact that people struggled to tell that something was, in fact, Internet-connected and essentially "smart" as these devices made their way into people's homes in a variety of formats. In the playdate scenario, P7 explained her concerns as a bystander:

"The Google Home and Amazon Alexa are controlled by awake words, they look like devices. That thing [smart toy], it goes back to the awareness factor. If I walked in, I would never know that is a smart toy. I don't know where it is going, I don't know what it is recording, I don't know if someone knows where my children are. That is when it gets concerning. Because those things like the Google Home and Alexa, people can track where you go. That [a smart toy] gets a child involved. That is where I get concerned as a bystander, I want to be aware of the things." (P7)

P7, who owned a few smart home devices, acknowledged that she did not know that the "dinosaur-shaped toy" was a smart toy. Given her prior knowledge regarding the tracking capability of similar voice assistant products, she would be concerned that her kids were accidentally exposed to another tracking device without her even knowing about it.

Awareness of device behaviors. Relatedly, bystanders also lack awareness of device behaviors and thus are not sure whether they are facing any risks or not. Nine participants (P2, P4, P6-9, P12, P14, P18) discussed this aspect. In the family cohabitant scenario, P6 shared her own story in her parents' house:

"My dad has a Google Home which, he doesn't use it to control music although sometimes it will, he might use it to ask a question about the weather or if we are having a conversation and he doesn't recall something he will ask the Google Home. It is kind of annoying when he isn't there, I unplug it because it is kind of weird like if we are talking just amongst ourselves and he says something vaguely like "okay Google" which is the activation thing, it will start listening and it is kind of weird. He works during the day so if I am there on the weekend. He has two one in his bedroom and one in his living room. I don't spend any time in his bedroom so I only unplug the living room one. I don't find the device useful and I don't know anything about it. I don't know if it is always on or whatever."

P6 was against the usage of Google Home in her parents' house. She chose not to expose herself in front of the Google Home by either unplugging the device or not staying in the same room

with the device as long as her father was not in the house. This was primarily due to her lack of awareness of the device capabilities and what the device might bring to her.

4.3 Privacy-Seeking Behaviors

The third aspect of bystanders' perceptions of smart homes is their privacy-seeking behaviors. Privacy-seeking behaviors refer to different ways people adopt to mitigate their privacy concerns and protect their privacy. Unlike the owners or users of smart home devices who directly set them up or turn them off the devices if they chose to, bystanders generally do not have access to directly control the devices, or simply do not believe that they should control the devices. In our study, several bystanders (P1, P4, P6, P9, P13, P15-16) mentioned a few ways of how they seek to protect their privacy. One common way in the temporary residency scenario was to cover the security camera if needed. In the family cohabitant scenario, P5 chose to place the voice assistant in a place where he only stayed to make food as a way to protect his privacy against the voice assistant.

In the playdate scenario, many bystanders mentioned that they would directly talk to the owners to either obtain more information about the toys or simply ask the owners to turn off the toys. However, bystanders also mentioned the potential caveat in doing so, as P1 stated:

"I feel like I am not in the place to be like "hey can you turn it off?", so I probably won't, but it still makes me feel uncomfortable." (P1)

This quote demonstrated that simple and direct privacy-seeking behaviors might create socially awkward situations. In this particular case, an awkward situation was caused by the perceived imbalanced power structure in the owner's home. As a result, bystanders ended up giving up seeking for privacy controls.

The three aspects discussed above, on the one hand, shape bystanders' privacy perceptions; on the other hand, provide insights into bystanders' privacy expectations in a variety of smart home contexts. Building on top of the above results, we present the findings from the follow-up co-design activity during which bystanders carried out various ideas to enact their privacy concerns and meet their privacy expectations.

4.4 Privacy Designs

In our study, we include a co-design activity to help us understand bystanders' desires in privacy controls and mitigation strategies. The activity provides a chance for researchers and bystanders to design together and cope with bystanders' privacy concerns. It is worth noting that although the designs are for a pre-defined smart home scenario, bystanders discussed the possibility of extending these designs to other scenarios.

We synthesize all designs and extract the design factors from our analysis. We first group all the factors based on design purposes, i.e., the privacy problems to be solved. We identify three purposes which can be mapped to the three aspects in bystanders' privacy perceptions, i.e., *expressing preferences* and *asking for device control* aiming to clarify bystanders' perceived norms; *detecting nearby devices* and *informing device behaviors* aiming to increase bystanders' awareness; as well as *limiting data collection* and *controlling data processing* aiming to empower bystanders with more control over their privacy.

We then conceptualize all design factors and purposes into two larger categories: cooperation mechanisms and bystander-centric mechanisms. Cooperation mechanisms refer to the designs that require communication between bystanders and owners to collaboratively resolve bystanders' privacy concerns, while bystander-centric mechanisms refer to the designs that require only bystanders' effort alone to meet their privacy expectations. The summary of the results can be

Table 2. Summary of bystanders' privacy design factors, organized based on design purposes and large categories.

Categories	Purposes	Factors
Cooperative mechanisms	Clarify norms	- Express preferences - Ask for device control
Bystander-centric mechanisms	Increase awareness	- Detect nearby devices - Inform device behaviors
	Provide controls	- Limit data collection - Control data processing

found in Table 2. It is worth noting that these design factors are not mutually exclusive. Many design ideas carried out by bystanders cover a few of these factors.

4.5 Cooperative Mechanisms

One primary reason for bystanders' concerns is the lack of communication between bystanders and owners. This is due to either the lack of communication channels or the potential social awkwardness and confrontation in face-to-face communication. Thus, bystanders' designs provide technological alternatives to enhance communication. Through effective communications, bystanders hope to establish or clarify contextual informational norms in the owners' smart home with respect for their privacy. From this perspective, seven participants considered the cooperative aspect in their designs, focusing on expressing their privacy preferences and asking for some device controls.

Express preferences. Seven bystanders (P1, P5-6, P9-10, P13-14) wished to express their privacy preferences to the owners through their designs. For example, in the playdate scenario, P5 designed an app interface in which he could specify his preferences regarding smart toys and other recording devices in the home. Once the preference was set, the owner would receive notifications in which the owner had the choice to either honor the preference by changing the smart toy settings or ignore the preference.

Ask for device control. Another cooperative element in bystanders' designs centers around asking for some controls of the devices in the owners' home. Six participants (P1-5, P10) included this aspect. Such designs provide a unique perspective in bystanders' privacy expectations since when discussing their perceptions, most bystanders acknowledged that they should not expect controls of others' devices. However, these privacy designs reflected that bystanders expected some controls over owners' devices to protect themselves. For example, P4 designed an app (Figure 1) to detect smart home devices in the owner's house. When he connected to the owner's home Wi-Fi, the app would provide a list of connected devices. If he was not comfortable with any of the listed devices and preferred for it to be turned off, he would make a request to the device directly through the app. The owner would be notified as well and would need to approve the request.

There are several insights behind this design. First, the app starts with a transparency feature that can detect all the devices connected in the home network so that bystanders are more aware of their environment. We will further unpack the awareness and transparency aspect in the Discussion section. Second, as a bystander, P4 prefers direct communication with the devices in the owners' home and the ability to turn the device on and off if needed as a way to protect his privacy. However, this idea can be considered as an intrusion for the owners, which further highlights the mismatch and tension between the owners and bystanders. Third, the fact that P4 designed an app to reflect his expectations of controlling the device rather than directly talking to the owner face-to-face

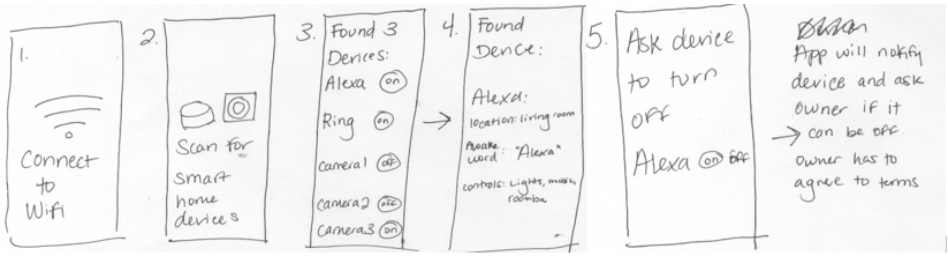

Fig. 1. The app design by P4.

suggests the potential of using our everyday technologies to avoid social confrontations in smart homes.

4.6 Bystander-Centric Mechanisms

The bystander-centric mechanisms refer to designs that only require effort from bystanders. Several bystanders' designs include many bystander-centric features, with a primary goal of addressing bystanders' concerns around the transparency issues in the owners' home as well as the lack of control of their data. More specifically, these designs focus on detecting nearby smart home devices, informing bystanders of device behaviors, limiting data collection, and controlling personal data process.

4.6.1 Device Awareness. Eleven of the designs (P1-8, P15-17) had a component to increase awareness of the smart devices in multiple ways. P4's example (Figure 1) from the previous section required bystanders to connect to the owners' home Wi-Fi to actively detect the existence of smart home devices inside the house. P14 designed the content of a text message, which included details regarding the types, schedule, and location of the devices. P8 designed an app that could help him realize the existence of a camera inside the owner's place, and if any devices existed, its operating status:

"You go into each room and the app lets you know if there's a security camera in their home. And going further, maybe it lets you know the location of every camera in the house. But that's dumb because then any burglar can do that. And it lets you know if it's on or off." (P8)

It is worth noting, however, that P8 also commented on the potential negative consequences of such an app: if he could use it, then any burglar could use it to detect the location of the cameras for a potential break-in. This concern was discussed in three groups, indicating that: (1) if such a design were to be implemented, more advanced security mechanisms should be included; and (2) bystanders' designs need to be critically examined by privacy and security experts as well as practitioners in order avoid security loopholes should any design idea be implemented.

4.6.2 Device behaviors. Bystanders also design with a desire to know the smart home devices' behaviors to make sure that they are informed. Eight designs (P1-2, P4, P7-8, P11, P17-18) included this feature. For example, one feature in P1's app design focused on improving the transparency of smart home devices, as he explained:

"I talked about an app, so it would be like an app that has access to all IoT devices in your home, so when you talked about the scenario if you walked in your friend's house and there was a camera and you weren't sure. If you walked up with an app, it would tell you all the devices they detected and the hours they are running, if it is on right now, who is using the device right now, the purpose of it so you are aware. This is for everyone around the device to know what it is used for." (P1)

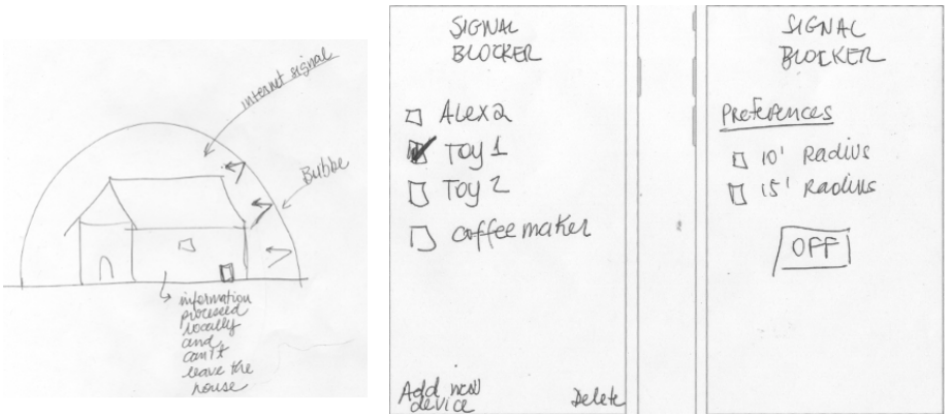

Fig. 2. The signal blocker designed by P10.

P1 was concerned that even if he noticed a smart home device, he would not be aware of the specific device's details. He would like the app to inform him about different aspects of these devices to increase his awareness, including the device status, purposes, schedule, etc. P7 designed a similar app to monitor device behaviors and inform him of any data collection. Besides, her design also had a piece for providing recommendations regarding how to avoid unwanted data collection. For example, in a case of security camera detection, the app would recommend, *"move to the kitchen if you don't want to be recorded, and don't say secrets."*

4.6.3 Limit data collection. Four designs (P3, P6, P7 P14) embedded a piece to limit data collection by smart home devices, particularly bystanders' data. For example, P6 designed an incognito mode for bystanders to alleviate concerns of being tracked:

"I know for a fact that some tech companies track your device's location so by default they track your location. And I think a feature in your smartphone that allowed you to go smart home incognito so if you go to your friends house, and they have a security camera that they don't turn off then I guess you have to get over that privacy concern but the max amount of privacy would be if you have this feature turned on in your phone, your whereabouts won't be in their system. That data doesn't mix with theirs." (P6)

P6 acknowledged the fact that she was tracked by technology companies, thus she designed an app for her smartphone in which she could set a "smart home incognito mode". Once activated, this mode could ensure that smart home devices would not track her.

Control data processing. Another feature is to control the processing of bystanders' data, including data sharing, access, storage, and deletion. Four designs (P3, P10, P13, P16) included this component. For example, P10 created a futuristic design which trapped the collected data inside the house (Figure 2):

"This is a signal blocker that stops information from leaving the house, kind of like bubbles around the house basically. Information can still get in. Signal blocker app will go along with it. I could get a notification that says 'Allow' or 'Deny' information to go out. Potentially it could add other people's devices to your signal blocker or they could share their system with me, kind of like Google Docs 'view', 'view and edit' link share." (P10)

P10s' design represented an entire smart home system as a signal block shield. In this design, the "bubble" referred to an invisible shield that stopped the information from going out. Bystanders could not control whether to use smart home devices or stop the data collection, but through the

app, they could potentially limit the collected data inside their friend's house. That would make P10 more comfortable.

P13's design of an app reflected the ideas of data deletion and storage. She explained:

"I would be happy if audio and video were deleted after a couple of days if the person went on and said I want to save this clip for this specific reason. Or if the data is only stored locally on their network or in the mesh network where it is connected between the devices itself or phone or computer. So it is not actually going outside of your home network and not being sent out anywhere so I know this data is not being shared or used maliciously." (P13)

P13's design reflected that her data would be properly handled by either smart home devices or the owners. By deleting the collected data after a certain amount of time and keeping the collected data stored in the owners' house, this app offered her peace of mind as a bystander since she would know that her data was secure.

It is worth noting that while our participants have different levels of experiences with smart homes, we do not observe notable differences between the designs of those who had more experiences and those with fewer experiences. We suspect this is due to 1) our small number of participants, 2) the qualitative nature of the study, and 3) our scenario-based discussions which reduces the potential influences of participants' prior experiences with smart home devices. We encourage future work to further dive into this issue using different methodologies (e.g., survey) with a larger sample size.

5 DISCUSSION

Few prior research has hinted the needs to study the privacy issues from other stakeholders in smart homes, such as visitors and other family members [24, 42, 47]. Our study attempted to respond to such needs. To the best of our knowledge, our work is the first of its kind that specifically focuses on the understudied bystanders' privacy in the context of smart homes, aiming to understand their privacy perceptions and desired ways of addressing their privacy concerns. Our results highlight the different aspects of shaping bystanders' privacy perceptions in smart homes. Besides, our co-design activity results in several design factors that the bystanders desire when designing privacy mechanisms to meet their privacy expectations in smart homes.

This study primarily focuses on smart home bystanders, while prior work primarily focuses on smart home users. Both groups are necessary and important stakeholders in smart homes and their perceptions and desirable design factors provide novel insights for the smart home industry, practitioners, and researchers. In this section, we compare our results to the findings from the literature (primarily the work of Zeng et al. [47], Zheng et al. [48], and Yao et al. [42]) to highlight major differences between the two groups. We choose these prior work because 1) they are among the pioneering work in understanding smart home users' privacy perceptions in the literature, and 2) they are similar to our work in terms of methodology. The goal of the comparison, instead of generating an exhaustive list of similarities and differences between bystanders and users, is to show that owners and bystanders may have different privacy needs. We also take the first attempt to answer the question posed by Yao et al. [42], i.e., "whose privacy should be protected and who should make the decision?"

5.1 Comparing Bystanders' and Users' Privacy Perceptions

Our results suggest that bystanders, despite their limited engagement with other people's smart homes, still hold their privacy concerns. We compare our findings of bystanders' privacy perceptions with other results of users' privacy perceptions and summarize three major differences: (1) contextual variations; (2) bystander's data access; and (3) privacy-seeking behaviors.

5.1.1 Contextual variations. Prior research on smart home users was mostly situated in their own homes. As a result, users' privacy perceptions were tied to their dwellings without too many variations. This means users chose to adopt smart home devices to accomplish certain goals in their home, such as home automation, surveillance, home safety, and remote access [47, 48]. As such, individual user's privacy perception centered around their specific use cases and was less likely to change once formed. In a sense, there is limited contextual variation from the users' perspective. In comparison, due to the nature of bystanders, they could switch their roles under different social relationships (e.g., family members living in the same home, visitors to another friend's home, or temporary renters of Airbnb homes). Thus, bystanders could face strong contextual variations. Our study showed that bystanders' privacy concerns varied in different scenarios and that their expectations and information needs were also significantly affected by many contextual factors, such as perceived social relationships with the owners and length of stay.

5.1.2 Expectation of bystanders' data access. Literature has discovered that users' mental models contained several entities that could access their data collected by smart home devices [47, 48]. These entities included device manufacturers, third-party advertisers, government, Internet service providers, etc. No evidence in the literature suggested that smart home users expected bystanders to obtain access to the collected data. However, bystanders from our study expected a certain level of control of either the users' devices or their data collected by these devices. Such expectation was perceived as reasonable by the bystanders as they were captured by the devices, and their privacy could be at risk.

5.1.3 Privacy-seeking behaviors. Literature has suggested that the majority of users did not seek privacy protection [47]. This was primarily due to users' overwhelming trust towards the device manufacturers. They believed that the manufacturers would provide satisfactory protection to their data and privacy. Even though users realized these privacy issues, many of them were not concerned about these issues and thus did not seek privacy protection [47]. Bystanders in our study, however, were somewhat different. On one hand, many bystanders claimed that they have taken some actions in their past experiences or in hypothetical scenarios, such as covering the security cameras, talking to the owners, etc. This was because bystanders' trust towards the owners as well as the mediators in some cases could cause privacy concerns, thus they would actively seek their privacy. On the other hand, we also noticed that some bystanders had concerns and would also like to seek protection, however, they did not do so due to the social pressure or awkwardness (e.g., not being in a place to directly talk to the owners), and they felt that there were no other options for privacy protections.

This comparison indicated several mismatches for privacy perceptions between the bystanders and the users/owners in smart homes. These mismatches highlight the fact that bystanders also have privacy needs and desire some controls, as well as the tension between bystanders and users in smart homes. The mismatches also point to potential opportunities for privacy designs to balance the privacy needs of both stakeholders. To answer the first part of the open question posed by Yao et al. [42] (i.e.,**"whose privacy should be protected"**), we argue that the privacy of both smart home users and smart home bystanders need to be well protected, since ignoring bystanders' privacy can heighten tensions between bystanders and owners, which would potentially change the social dynamics at the home. In the long run, there can also be various push backs for the adoption and use of these devices across a variety of contexts.

5.2 Unpacking Bystanders' Privacy Designs

The co-design activity in our study results in several design factors that bystanders desire to mitiga te their privacy concerns. In this section, we would like to take a deeper look at these design factors to illuminate future privacy designs for smart homes.

5.2.1 Cooperative mechanisms. **Rationale.** In our study, bystanders' privacy perceptions changed across different scenarios. However, as we noted before, the norms were not always clear in different contexts, especially when considering various social factors embedded in those contexts. Thus, bystanders often desired to cooperate and even negotiate with the owners/users regarding their privacy in a given context. For example, when bystanders did not give consent for their voice to be recorded, they hoped to send a request to the owners and ask for approval to limit the audio recording. As Nissenbaum argues in the theory of Contextual Integrity, it is important to understand the contextual information norm to decide whether one's privacy is breached within a given context [30, 31]. This contextual information norm includes three independent parameters: (1) actors, including the subject, sender, recipient, embody the context; (2) information types, i.e., the types of information that are collected; and (3) transmission principles, i.e., the principle that is either socially acknowledged or required by law [30, 31]. From the bystanders' perspectives, once the *actors* are determined, they would like to explicitly express their privacy preferences to specify *information types*. Considering the *transmission principle* in the smart home, bystanders further sought users' approval for device controls instead of directly controlling the devices at their command. Thus, through communication and potential negotiation between bystanders and users, the cooperative mechanisms were designed to clarify the contextual information norm in smart homes which were not always clear, so that bystanders' privacy expectations could be better achieved.

Comparison among cooperative mechanisms. In the literature, the attempt to cooperatively negotiate privacy management has been made in several contexts to enact the privacy needs of different stakeholders. For example, in the context of photo tagging on Facebook, to protect the privacy of users who were tagged in photos and, at the same time, still make the photo-sharing and tagging possible for the photo owners, Besmer and Lipford proposed a design which allowed the tagged users to send the photo owner a request and ask that if they were tagged in the photo, the photo should be hidden from certain people [5]. Xu et al. proposed the design principle for privacy-enhancing tools, which stated that users should act as a member of a group and have collective control of their information [41]. In the context of drones, Yao et al. proposed two mechanisms with a cooperative nature: Deletion Request (i.e., drone bystanders could send request to the controllers to delete their footage) and Controller-Bystander App (i.e., drone bystanders could obtain more information of and, if needed, communicate with the drone controllers) [45]. Both these two mechanisms were designed to enact the privacy issues of drone bystanders but at the same time, balance the privacy needs of drone bystanders and the functional needs of drone controllers.

In our research, the cooperative mechanisms were mostly similar to those mechanisms mentioned above. For example, P4's design asking for device control was similar to the Controller-Bystander App in the context of drone privacy designs [45], and P5's design to express his privacy preferences was similar to the photo tagging tools [5]. It is worth noting that, despite being largely embraced by the researchers as well as targeted users [5, 45], most of these cooperative mechanisms have not been implemented in the real world. This is in part due to the feasibility of these mechanisms, which have either technological barriers or policy obstacles, as well as many other potential design issues, e.g., different preferences of drone controllers and bystanders, the amount of user effort required in cooperation, etc. In our study, we also anticipate similar feasibility issues and design

questions, such as whether bystanders have different privacy needs than the owners/users and if the bystanders' privacy needs to defeat the purposes of owners' smart home devices. However, the recent large adoption of Amazon Echo in hotel rooms [9] indicates the urgency of effective privacy mechanisms for bystanders. We advocate that future research should look deep into these issues, examine user-generated ideas more comprehensively in terms of feasibility, usability, and other potential issues (e.g., required user efforts), then propose new cooperative mechanisms to better suit the needs of both smart home users/owners and bystanders.

5.2.2 Bystander-Centric mechanisms. **Designing for awareness.** The other set of design factors focused on bystanders only, with a primary focus on increasing awareness and transparency as well as providing some controls to bystanders. On one hand, as notice and choice are well-recognized privacy principles, increasing bystanders' awareness of nearby devices and device behaviors reduce their uncertainty and alleviate their privacy concerns to a certain degree. On the other hand, what level of awareness should be provided to bystanders and how to do so remain open questions and require further investigation, especially when considering if such awareness tools fall into the wrong hands and cause unpleasant safety incidents. For example, P8's design provided awareness to the bystanders by showing them the location of every security camera in the house, but at the same time, if this app was accessed by burglars, then the safety of the house might be compromised. Future research is needed to provide better and more comprehensive solutions.

Designing for control. In terms of controls, we found it intriguing that bystanders designed for having active controls on other people's property, even though the controls were towards bystanders' data rather than the users' devices. This was an indicator to us that bystanders also expected to have agency in other people's homes. However, it is worth noting that, while providing some agency to bystanders could potentially help them to be able to better control their data from being collected and shared, this could conflict with the owners/users' purpose of using the devices or even invade the users' privacy. For example, P10's design of the signal blocker limited the data being shared with entities outside of the house but also potentially interfere with the owner's data as all data was collected by the same devices.

5.2.3 Comparisons bystanders' and users' privacy designs. In the end, we also make a comparison between bystanders' design factors in our research and the owners/users' design factors in Yao et al.'s study [42]. We found that although the design features (e.g., information device behaviors, local data storage) under the bystander-centric mechanisms category in our study were similar to the ones in their study, the design features under the cooperative mechanisms category were unique. As discussed before, the cooperative mechanisms aimed to enhance the communication between bystanders and owners/users so that they could negotiate and hopefully fulfill their individual privacy needs. To answer the second part of the question posed by Yao et al. [42] (i.e., "**who should make the decision**"), we argue that such decisions should be made cooperatively between end-users and bystanders with a consideration of the specific context they are in.

5.3 Design Implications

Privacy in smart homes is an important topic in the CSCW community. Many studies have looked at the privacy concerns and perceptions of the owners/users regarding smart homes as a whole [47, 48] and individual smart home devices [24, 27], as well as users' desired ways of mitigating their privacy concerns [42]. Nevertheless, all of these studies hinted at potentially different privacy perceptions from the bystanders' perspective, yet none of these studies have explored the differences. Our study provides rich and novel empirical evidence demonstrating that 1) bystanders in smart homes have various privacy concerns which are further influenced by several contextual factors, and 2) bystanders desire some forms of privacy controls. Our discussion also dives into the mismatches

between the perceptions of bystanders and owners/users, highlighting the tension between these two stakeholders and the needs for enact privacy issues cooperatively.

Based on our study results, we make the following concrete design suggestions for future privacy-enhancing mechanisms in smart homes.

Transparency. In various smart home application contexts, the existence of smart home devices, as well as their behaviors, should be more transparent to bystanders. For example, in the temporary residency scenario, one concrete example is that the owners should proactively provide information about smart home devices, such as their location, purposes, whether data is collected and stored, etc. In the case that the owners do not know some of this information themselves, the device manufacturers should provide this information along with the device, e.g., in a poster with a QR code. The owners can potentially place physical signs alongside the smart home devices in the apartment so that the tenants are more aware of such devices, and provide the tenants with options to opt-out from these devices being used. In the case where mediators exist (e.g., Airbnb in the temporary residency scenario), the mediators can also assure by notifying bystanders if the owners delete their recordings.

Expressing preferences. When designing privacy mechanisms in smart homes, it is critical to consider the needs of both owners/users and bystanders collaboratively to design for both groups. For example, smart home device platforms (e.g., Samsung SmartThings) can potentially create apps for both owners/users and bystanders so that the latter can express their preferences and potentially communicate with owners/users.

Different modes. Smart home devices owner/users and the devices themselves should also be proactive in considering and protecting bystanders' privacy in various ways. One concrete solution is for smart home devices to have different modes. The devices will be fully functional in user mode, but in bystander mode, the devices' functions can be selectively disabled. For example, the voice assistants will stop recording if a different voice is detected, indicating the possibility of friends visiting; the security camera will only record footage of a designated area in an Airbnb apartment (e.g., the hallway), ensuring the safety of the apartment while protecting tenants' privacy.

It is worth noting that the design suggestions above focus primarily on bystanders. However, one open question to ask for future research is, *how will these mechanisms benefit the owners/users and other stakeholders (e.g., mediators) and whether they will accept these mechanisms?* Grudin's prior work on groupware argued that people who used groupware would not benefit the most, and in some cases, technology that was designed to support one group of people might negatively impact another [18]. Thus, ensuring these privacy mechanisms also benefits owners and other stakeholders are crucial for their adoption.

5.4 Limitations and Future Work

Our study is the first to explicitly focus on understanding how bystanders perceive their privacy in smart homes and their desired ways of mitigating their concerns. As such, our exploratory approach has a few limitations.

First, our three scenarios in the study were by no means exhaustive in terms of different application contexts of smart homes and the types of bystanders. Other example scenarios and bystanders could include, for example, a UPS delivery man being caught by a smart doorbell every day, or children being caught by security cameras in their neighbors' house. Future research can either investigate a more diverse set of scenarios or come up with different contextual factors so that participants can assemble their scenarios.

Second, given the purpose and the exploratory nature of the study, our focus group and the co-design activity only included a bystanders' perspective. The co-design activity, although insightful, was also limited by the duration of the study. Future research can consider running extended

participatory design workshops with owners/users, bystanders and other potential stakeholders (e.g., developers) to surface the tension and gain a more holistic understanding of their perceptions and desired designs.

Third, given the scope of this study, we did not critically evaluate bystanders' designs in terms of their usability, feasibility, and potential consequences. Future research can focus more on critical evaluation of the designs emerged from our study as well as prior studies [42] and come up with new designs to better fulfill the needs of different stakeholders.

6 CONCLUSION

Prior literature in smart home privacy has focused on end-users, leaving other potential stakeholders, such as bystanders, understudied. In this study, we focus on smart home bystanders, i.e., people who are not the owners/users of these devices but can potentially be involved in the use of such devices. We aim to understand bystanders' privacy perceptions in various contexts and their desired ways to mitigate their privacy concerns. Through six focus groups with 18 participants, our study results in a number of contextual factors that can potentially influence bystanders' privacy perceptions of smart homes. In addition, we also identify a set of design factors that the bystanders consider in their desirable privacy mechanisms to address their concerns. These factors can further be categorized into two types, i.e., cooperative mechanisms and bystander-centric mechanisms. Our research highlights bystanders' needs for privacy and some means of controls, the tension between smart homeowners/users and bystanders, as well as how cooperative mechanisms can be used to better support and balance the needs of both groups. We propose several concrete design suggestions based on our results, i.e., having both owners/user-oriented apps and bystander-oriented apps in smart home platforms.

7 ACKNOWLEDGEMENT

We thank our participants for their experiences and insights. We are also very grateful to Bryan Semaan, Nata Barbosa, Smirity Kaushik for their assistance as well as the anonymous reviewers for their thoughful feedback. This work was supported in part by NSF Grant CNS #1464347.

REFERENCES

[1] Noah Apthorpe, Dillon Reisman, and Nick Feamster. 2017. A smart home is no castle: Privacy vulnerabilities of encrypted IoT traffic. *arXiv preprint arXiv:1705.06805* (2017).

[2] Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster. 2017. Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic. *arXiv preprint arXiv:1708.05044* (2017).

[3] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *arXiv preprint arXiv:1805.06031* (2018).

[4] Abdullahi Arabo, Ian Brown, and Fadi El-Moussa. 2012. Privacy in the age of mobility and smart devices in smart homes. In *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)*. IEEE, 819–826.

[5] Andrew Besmer and Heather Richter Lipford. 2010. Moving beyond untagging: photo privacy in a tagged world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1563–1572.

[6] Richard E Boyatzis. 1998. *Transforming qualitative information: Thematic analysis and code development*. sage.

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

[8] Antorweep Chakravorty, Tomasz Wlodarczyk, and Chunming Rong. 2013. Privacy preserving data analytics for smart homes. In *Security and Privacy Workshops (SPW), 2013 IEEE*. IEEE, 23–27.

[9] Andria Cheng. 2018. Amazon-Marriott Deal Will Make Alexa A Hotel Butler, But The Implications Range Far Wider. (Jun 2018). https://www.forbes.com/sites/andriacheng/2018/06/19/amazons-marriott-deal-is-way-beyond-alexa-as-your-new-hotel-butler/#22b53db9721e

[10] Federal Trade Commission et al. 2015. Internet of Things: Privacy & security in a connected world. *Washington, DC: Federal Trade Commission* (2015).

[11] Anupam Das, Martin Degeling, Daniel Smullen, and Norman Sadeh. 2018. Personalized Privacy Assistants for the Internet of Things. (2018).
[12] Trisha Datta, Noah Apthorpe, and Nick Feamster. 2018. A Developer-Friendly Library for Smart Home IoT Privacy-Preserving Traffic Obfuscation. In *Proceedings of the 2018 Workshop on IoT Security and Privacy*. ACM, 43–48.
[13] 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, 2377–2386.
[14] Emily Dixon. 2019. Family finds hidden camera livestreaming from their Airbnb in Ireland. (Apr 2019). https://www.cnn.com/2019/04/05/europe/ireland-airbnb-hidden-camera-scli-intl/index.html
[15] Joseph L Fleiss, Bruce Levin, and Myunghee Cho Paik. 2013. *Statistical methods for rates and proportions*. John Wiley & Sons.
[16] Geoffrey A. Fowler. 2015. Talking Toys Are Getting Smarter: Should We Be Worried? (Dec 2015). https://www.wsj.com/articles/talking-toys-are-getting-smarter-should-we-be-worried-1450378215
[17] Sidney Fussell. 2019. Airbnb Has a Hidden-Camera Problem. (Mar 2019). https://www.theatlantic.com/technology/archive/2019/03/what-happens-when-you-find-cameras-your-airbnb/585007/
[18] Jonathan Grudin. 1994. Computer-supported cooperative work: History and focus. *Computer* 27, 5 (1994), 19–26.
[19] Roberto Hoyle, Robert Templeman, Denise Anthony, David Crandall, and Apu Kapadia. 2015. Sensitive Lifelogs: A Privacy Analysis of Photos from Wearable Cameras. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 1645–1648.
[20] 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 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 571–582.
[21] Andreas Jacobsson, Martin Boldt, and Bengt Carlsson. 2016. A risk analysis of a smart home automation system. *Future Generation Computer Systems* 56 (2016), 719–733.
[22] Timo Jakobi, Gunnar Stevens, Nico Castelli, Corinna Ogonowski, Florian Schaub, Nils Vindice, Dave Randall, Peter Tolmie, and Volker Wulf. 2018. Evolving Needs in IoT Control and Accountability: A Longitudinal Study on Smart Home Intelligibility. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 4 (2018), 171.
[23] Li Jiang, Da-You Liu, and Bo Yang. 2004. Smart home research. In *Machine Learning and Cybernetics, 2004. Proceedings of 2004 International Conference on*, Vol. 2. IEEE, 659–663.
[24] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. In *Pro. ACM Human-Computer Interaction CSCW*. ACM.
[25] Huichen Lin and Neil W Bergmann. 2016. IoT privacy and security challenges for smart home environments. *Information* 7, 3 (2016), 44.
[26] Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. 2018. "What Can't Data Be Used For?" Privacy Expectations about Smart TVs in the US. *European Workshop on Usable Security (EuroUSEC)* (2018).
[27] 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*. ACM, 5197–5207.
[28] Simon Moncrieff, Svetha Venkatesh, and Geoff West. 2007. Dynamic privacy in a smart house environment. In *Multimedia and Expo, 2007 IEEE International Conference on*. IEEE, 2034–2037.
[29] Nata M. Barbosa, Joon S. Park, Yaxing Yao, and Yang Wang. 2019. "What if?" Predicting Individual Users' Smart Home Privacy Preferences and Their Changes. *Proceedings on Privacy Enhancing Technologies (PoPETS)* 4 (2019), 211–231.
[30] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Washington law review* 79, 1 (2004), 119–158.
[31] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
[32] Erika Shehan Poole, Marshini Chetty, Rebecca E Grinter, and W Keith Edwards. 2008. More than meets the eye: transforming the user experience of home network management. In *Proceedings of the 7th ACM conference on Designing interactive systems*. ACM, 455–464.
[33] Elizabeth B-N Sanders and Pieter Jan Stappers. 2008. Co-creation and the new landscapes of design. *Co-design* 4, 1 (2008), 5–18.
[34] Marc Steen, Menno Manschot, and Nicole De Koning. 2011. Benefits of co-design in service design projects. *International Journal of Design* 5, 2 (2011).
[35] Froukje Sleeswijk Visser, Pieter Jan Stappers, Remko Van der Lugt, and Elizabeth BN Sanders. 2005. Contextmapping: experiences from practice. *CoDesign* 1, 2 (2005), 119–149.
[36] James Vlahos. 2019. Smart talking: are our devices threatening our privacy? (Mar 2019). https://www.theguardian.com/technology/2019/mar/26/smart-talking-are-our-devices-threatening-our-privacy

[37] Junjue Wang, Brandon Amos, Anupam Das, Padmanabhan Pillai, Norman Sadeh, and Mahadev Satyanarayanan. 2018. Enabling Live Video Analytics with a Scalable and Privacy-Aware Framework. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)* 14, 3s (2018), 64.

[38] Yang Wang, Huichuan Xia, Yaxing Yao, and Yun Huang. 2016. Flying Eyes and Hidden Controllers: A Qualitative Study of People's Privacy Perceptions of Civilian Drones in The US. *Proceedings on Privacy Enhancing Technologies* 2016, 3 (2016), 172–190.

[39] Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM, 11:1–11:16.

[40] Peter Worthy, Ben Matthews, and Stephen Viller. 2016. Trust me: doubts and concerns living with the Internet of Things. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*. ACM, 427–434.

[41] Heng Xu, Robert E Crossler, and France BéLanger. 2012. A value sensitive design investigation of privacy enhancing tools in web browsers. *Decision support systems* 54, 1 (2012), 424–433.

[42] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. (2019).

[43] Yaxing Yao, Davide Lo Re, and Yang Wang. 2017. Folk Models of Online Behavioral Advertising. In *Proceedings of the Computer Supported Cooperative Work (CSCW)*. ACM.

[44] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. Free to Fly in Public Spaces: Drone Controllers' Privacy Perceptions and Practices. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 6789–6793.

[45] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 6777–6788.

[46] Kenji Yoshigoe, Wei Dai, Melissa Abramson, and Alexander Jacobs. 2015. Overcoming invasion of privacy in smart home environment with synthetic packet injection. In *TRON Symposium (TRONSHOW), 2015*. IEEE, 1–7.

[47] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security & Privacy Concerns with Smart Homes. In *Symposium on Usable Privacy and Security (SOUPS)*.

[48] Serena Zheng, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Privacy in Smart Homes. *arXiv preprint arXiv:1802.08182* (2018).

[49] 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. *Mensch und Computer 2018-Workshopband* (2018).

A APPENDIX

Table 3. Full list of participants' perceived benefits of smart homes

Group	Participants	Perceived pros/benefits	Perceived cons/risks
1	P1	Convenient (e.g., playing music); cool	Device could go off sometimes (e.g., Amazon Echo started to play music by itself); lack of data control
	P2	Quick access to easy tasks (e.g., turning off living room lights)	Device not functioning properly due to the lack of power (e.g., smart locks would be tough to deal with if the power went off)
	P3	Convenient (e.g., checking local weather quickly)	Security camera caused significant privacy concerns; no concern if consent was granted, but would have privacy concerns if no consent was provided
2	P4	Providing proof for law enforcement (e.g., Amazon Echo recorded the process of a murder case)	The more you put on technology, the more vulnerable you become; lack of regulations on smart home devices usage
	P5	Ensuring home safety (e.g., remote access through security camera and record break-ins); convenient; cool	Smart home could take over the house and do crazy things (e.g., let burglar come in)
	P6	Cool (e.g., interacting with Google Home was very futuristic)	Potential data sharing among multiple users of the same devices (e.g., roommate); long term impact on people's acceptance of data collection
3	P7	Convenient (e.g., playing music on Spotify through Amazon Echo)	Users' habits were not formed (e.g., she only used Amazon Echo to play music)
	P8	Made home more accessible (e.g., proving convenience for people with disability)	Could be privacy intrusive for people with disabilities (e.g., blind users could not know the running status of the security camera); lack of awareness in general
	P9	Home automation made some tasks easier (e.g., smart coffee maker could be controlled by the phone to make coffee)	Security camera could be very intrusive and record every single move; security camera could be hidden

	P10	Convenient (e.g., voice communication with Amazon Echo to check the package status)	Had a long learning curve (e.g., he had to learn how to use the devices through YouTube videos)
4	P11	Ensuring home safety (e.g., making emergency calls through Amazon Echo)	Expensive
	P12	Easy connection with other family members (e.g., using Amazon Show)	Expensive; manufacturers could collect and abuse data
5	P13	Convenient (e.g., making calls through voice assistant); ensuring home safety (e.g., outdoor security camera sending images to her phone)	Device malfunction (e.g., outdoor security cameras got cut off)
	P14	Easy connection with other family members and ensuring in-home safety (e.g., sharing live videos through security camera app so that other family members could see him if he fell)	Privacy concerns (e.g., sharing the videos all the time); Internet connection could be difficult for people who stayed at the senior citizen centers
	P15	Convenient (e.g., let people come into the house using smartphone)	Security risks (e.g., hacking the phone and getting access to the house)
6	P16	Convenient (e.g., playing music)	Privacy concerns (e.g., building profiles)
	P17	Convenient (e.g., making calls, remotely monitoring kids and pets at home)	Lack of trust towards big companies (e.g., skeptical towards Amazon Echo's policy regarding deleting the audios after 45s)
	P18	Safer than the Internet; convenient	Expensive; lack of trust towards manufacturers (e.g., smart home devices made by small manufacturers might have less data protection measures)

Received April 2019; revised June 2019; accepted August 2019